Mikko Koskinen

Varmuuskopiointipalvelun suunnittelu ja toteutus

Opinnäytetyö
Tieto- ja viestintätekniikka

2017

Kaakkois-Suomen ammattikorkeakoulu

Kaakkois-Suomen ammattikorkeakoulu

Tekijä/Tekijät	Tutkinto	Aika
Mikko Koskinen	Insinööri (AMK)	Joulukuu 2017

Opinnäytetyön nimi

40 sivua
10 liitesivua

Varmuuskopiointipalvelun suunnittelu ja toteutus

Toimeksiantaja

Kahviduuri Ay

Ohjaaja

Martti Kettunen

Tiivistelmä

Tämän opinnäytetyön tarkoituksena on suunnitella ja toteuttaa varmuuskopiointipalvelu kotkalaiselle ICT-alan yritykselle. Palvelulla on tarkoitus tuottaa asiakasyritykselle luotettava, vikasietoinen ja helppokäyttöinen varmuuskopiointi, jossa tiedot ovat myös helposti palautettavissa.

Varmuuskopiointi on erittäin tärkeä osa nykyaikaista tiedonhallintaa ja se kuuluu yrityksen tietoturvaan. Ajantasaisella varmuuskopiolla voidaan palauttaa yrityksen tila nopeasti onnettomuuden tai haittaohjelman aiheuttaman tiedon menetyksen jälkeen. Tiedostojen nopea palauttaminen tiedon hävittyä voi jopa pelastaa yrityksen konkurssilta.

Työ aloitettiin tutkimalla varmuuskopioinnin teoriaa sekä vertailemalla erilaisia varmuuskopiointimenetelmiä ja -välineitä, pilvipalveluita sekä suosituimpia ilmaisia varmuuskopiointiohjelmia. Vertailu tapahtui teoreettisesti sekä virtualisoidussa ympäristössä tehdyllä käytännön kokeilulla. Vertailun jälkeen muodostettiin varmuuskopiointipalvelu valitsemalla siihen parhaiten sopivat menetelmät, välineet ja ohjelmistot. Varmuuskopiointipalveluun tehtiin myös yksityiskohtaiset asennus- ja käyttöönotto-ohjeet.

Varmuuskopiointiohjelmaksi valittiin Cobian Backup sekä menetelmäksi joko täysvarmistus tai täysvarmistus yhdistettynä lisäys- tai eroavuusvarmistukseen. Varmuuskopiointi suoritetaan päivittäin suoraan NAS-palvelimelle ja sieltä Mega:n pilvitallennustilaan. Vaihtoehtoisesti pilvenä voidaan käyttää jo yrityksellä olemassa olevaa palvelua. Lisävarmennuksia voidaan ottaa ajoittain ulkoiselle kovalevylle ja järjestelmän vikasietoisuutta voidaan parantaa lisäämällä toinen NAS-palvelin, peilattuja kovalevyjä tietokoneisiin tai UPS-laitteita.

Varmuuskopioinnin järjestäminen vaatii hieman vaivannäköä ja mahdollisesti rahallista panostusta, mutta hyvin toteutettuna voi säästää hyvin suurelta tietomenetykseltä ja rahalliselta tappiolta.

Asiasanat

eroavuusvarmistus, lisäysvarmistus, palauttaminen, pilvipalvelu, täysvarmistus, varmuuskopiointi

South-Eastern Finland University of Applied Sciences

Author (authors)	Degree	Time
Mikko Koskinen	Bachelor of Information Technology	December 2017
Thesis title Designing and implementing a backup service		40 pages 10 pages of appendices
Commissioned by Kahviduuri Ay		
Supervisor Martti Kettunen		

Abstract

The goal of this thesis was to design and implement a backup service. The backup service should provide reliable, fault-tolerant and easy-to-use data backup for a customer. It should also feature easy data recovery. Data backup is a critical component of modern information management and it is part of information security. It is possible to recover from an accidental data loss or malware with up-to-date backup. Fast recovery from disaster can even save a company from bankruptcy.

The thesis was started by studying the theory of backup and comparing different backup methods and tools, cloud services and few freeware backup applications. The method comparison was done theoretically while backup software was tested in virtualized environment. The backup service was then built using selected methods and tools. Part of this thesis was also detailed installation and implementation instructions for the backup service.

Cobian Backup was chosen to be used in the backup service and a full backup solely or a full backup and incremental or differential backup will be used as a backup method. The backup will be taken daily to a network attached storage where it will be uploaded to Mega cloud storage. If a customer has existing cloud storage, it can be used instead. To make the backup service more reliable, one should add second NAS, use mirrored hard disks on computers or apply UPS-systems to ensure electricity.

Making a backup plan for a company requires some inverment of money and work but when executed properly it can save one from massive information and financial loss.

Keywords

Backup, network attached storage, full backup, incremental, differential, recover

SISÄLLYS

KÄSITTEET JA LYHENTEET

Archive bit Arkistointimääre

FREEWARE Ilmaisohjelma.

HDD (Hard Disk Drive) Perinteinen kovalevy.

NAS (Network Access Storage) Tallennusjärjestelmä, joka jakaa siihen kytketyt kovalevyt verkossa yhteiskäyttöön.

Open source Avoin lähdekoodi.

SAN (Storage Area Network) Verkko, joka yhdistää tiedostopalvelimien yhdistäminen niitä käyttäviin palvelimiin.

SDD (Solid State Drive) Flash-muistiin perustuva kovalevy.

Shadow Copy Microsoft Windows -järjestelmään integroitu teknologia, joka sallii tiedostojen tai loogisten levyjen varmuuskopioimisen niiden ollessa käytössä.

RAID (Reduntant Array of Independent Disks) Tekniikka, joka yhdistää useita erillisiä kiintolevyjä yhdeksi loogiseksi levyksi.

UPS (Uninterruptible Power Supply) Järjestelmä tai laite, joka takaa tasaisen virransyötön lyhyiden katkosten tai syöttöjännitteen epätasaisuuksien aikana.

1 JOHDANTO

Tämän opinnäytetyön tavoitteena on suunnitella ja toteuttaa varmuuskopiointipalvelu Kahviduuri Ay:lle. Työ toteutettiin kokonaisuudessaan vuoden 2017 aikana. Varmuuskopiointipalvelu on tarkoitus ottaa yrityksen käyttöön sen valmistuessa. Vastaavanlaista varmuuskopiointipalvelua on selvitetty Jyväskylän ammattikorkeakoulussa vuonna 2011 Antti Immosen opinnäytetyössä ”Varmuuskopiointipalvelu”.

Opinnäytetyön toimeksiantaja on kotkalainen ICT-alan palveluita tuottava Kahviduuri Ay. Yritys työllistää kaksi henkilöä ja se tuottaa monenlaisia palveluja mukaan lukien tietokoneen huollot, viruspoistot, järjestelmän optimoinnit, datan palautukset, komponenttien vaihdot ja asennukset sekä käyttöjärjestelmäasennukset (Kahviduuri. 2017.)

Varmuuskopiointi on kriittinen osa nykyaikaista tiedonhallintaa. Yritykset tuottavat ja säilyttävät entistä enemmän kriittistä dataa omissa järjestelmissään. Tämän datan häviäminen voi tuottaa valtavia tappioita ja jopa aiheuttaa yrityksen kaatumisen.

Opinnäytetyön tavoitteena on luoda Kahviduuri Ay:lle varmuuskopiointipalvelu, jota yritys tarjoaa asiakkailleen. Sen tulee olla helppokäyttöinen ja luotettava sekä hyvin yksilöllisesti asiakkaan tarpeisiin ja ympäristöön mukautuva. Mukaan tulee voida lisätä pilvitallennustila sekä tarvittava määrä ulkoista tallennustilaa.

Opinnäytetyössä selvitetään erilaisten tallennusmedioiden sopivuutta Kahviduuri Ay:n varmuuskopiointipalvelun tarpeisiin. Lisäksi selvitetään erilaisten tallennusmenetelmien ja varmuuskopiointiohjelmien sopivuutta palveluun. Työ koostuu kahdesta vaiheesta, josta ensimmäisessä tutkitaan varmuuskopioinnin teoriaa ja toisessa testataan erilaisia varmuuskopiointiohjelmia ja -menetelmiä. Näistä sopivimmat valitaan uuteen palveluun.

2 VARMUUSKOPIOINTI

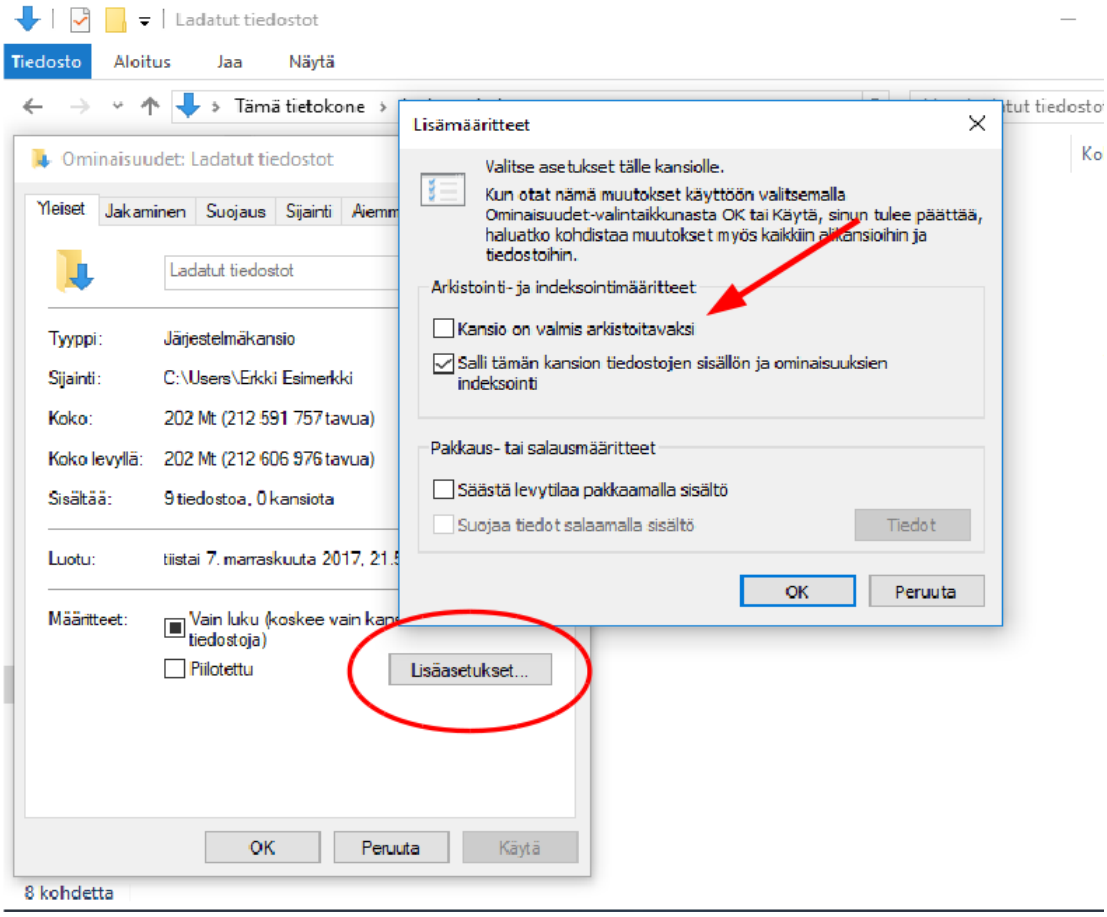
Varmuuskopioinnilla tarkoitetaan käytännössä tiedon kopioimista alkuperäisestä lähteestä muualle, niin että se voidaan palauttaa tai ottaa käyttöön alkuperäisten tietojen hävitessä. Tieto voi hävitä onnettomuuden, laiterikon tai vahingon seurauksena. (Jaakohuhta 2011, 62.)

Varmuuskopiointi on myös tärkeä osa tietoturvaa. Verkkorikollisuus on kasvanut ja viime vuosina erityisesti kiristysohjelmat (ransomware) ovat yleistyneet verkkorikollisten käytössä. Kiristysohjelma salaa tietokoneen tärkeät tiedostot tai jopa kokonaisen kovalevyn ja vaatii rahaa salauksen purkuavaimesta. Poliisin, F-Securen ja Viestintäviraston luomalla ransomware-sivustolla kerrotaan, ettei salattuja tiedostoja käytännössä voida avata ilman avainta (Ransomware 2017). Ainoa tapa palauttaa haittaohjelman salaamat tiedostot on ajantasainen varmuuskopio.

Arkistointi sekoitetaan usein varmuuskopiointiin vaikka ne tarkoittavat eri asioita. Varmuuskopion ollessa palautettavissa oleva kopio tiedostoista, arkistoinnilla tarkoitetaan tiedon pidempiaikaista säilytystä. Arkistoitua tietoa ei voi palauttaa samalla tavalla kuin varmuuskopioitua. Yleensä tietoa josta voi vielä joskus olla hyötyä, mutta jota ei aktiivisesti tarvita, voidaan arkistoida. Parhaiten arkistointi sopii esimerkiksi dokumenttien, sähköpostien ja vanhojen tietokantojen säilyttämiseen. (SearchDataBackup: What is data archiving? 2015.)

2.1 Arkistointimääre

Arkistointimääre (arkistointibitti, archive bit) on bitti, jolla Windows-järjestelmä merkitsee varmuuskopioitavat tiedostot niiden luomisen ja muuttamisen yhteydessä (Kuva 1). Varmuuskopioitaessa merkitään arkistoiduksi täys- ja lisäysvarmistuksen yhteydessä ja sen merkinnästä vastaa varmistusohjelma. Arkistointimäärettä tarvitaan eroavuus- tai lisäysvarmistuksen yhteydessä, jolloin varmistusohjelma tarkastaa onko tiedostoa muutettu tai kopioitu edellisen varmuuskopioinnin jälkeen. Mac- ja Linux-käyttöjärjestelmät eivät käytä arkistointimäärettä, vaan perustavat varmuuskopiointinsa tiedostoihin sidottuihin aikaleimoihin. (Jaakohuhta 2011, 45.)



Kuva 1. Arkistointimääre Windows 10 -käyttöjärjestelmässä

2.2 Varmuuskopiointi menetelmät

Varmuuskopiointi voidaan suorittaa monella eri tavalla. Eri menetelmät voidaan luokitella sen perusteella mitä dataa varmuuskopiossa ja järjestelmässä on tai millä tavalla varmuuskopiointi on tehty. Yleisimmin käytetyt menetelmät ovat täysi varmuuskopiointi (Full backup), lisäysvarmistus (Incremental backup) ja eroavuusvarmistus (Differential backup). Lisäksi varmuuskopioista voidaan käyttää, niiden ja järjestelmän tiedostojen välisen aikaeron mukaan, online, near-line ja offline termejä. (Sanastokeskus TSK ry 2010b; Rao & Nayak 2014, 264 - 265.)

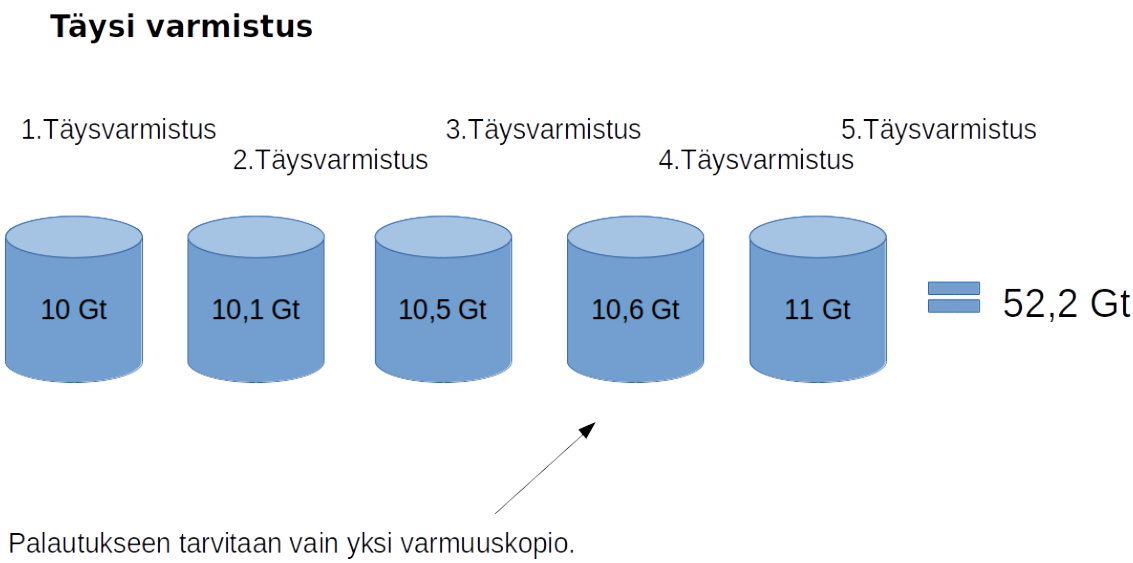
2.2.1 Täysi varmuuskopiointi

Täysi varmuuskopiointi, full backup tai täysvarmistus tarkoittaa nimensä mukaisesti täydellistä kopiota koko datasta. Täysvarmistuksen aikana tiedostojen arkistointimääre asetetaan pois päältä jotta seuraava varmuuskopiointi ei var-

mista jo varmistettuja tiedostoja. Täysvarmistusta käytetään aina ensimmäistä kertaa varmuuskopiota tehdessä. Täysvarmistuksen koko on suurempi kuin muiden varmuuskopiointimenetelmien ja sen ottaminen kestää pidempään (kuva 2). (Sanastokeskus TSK ry 2010a; Backup4all 2012c, Jaakohuhta 2011, 245.)

Täysi varmuuskopiointi on tarkasteltavista menetelmistä kaikkein kattavin. Se varmuuskopioi kaikki valitut tiedostot ja kansiot, jolloin jo yhdellä täydellä varmuuskopioinnilla voidaan palauttaa esimerkiksi yrityksen koko tiedostojärjestelmä. Täysi varmuuskopiointi on tiedon varmennuksen kannalta kaikkein paras vaihtoehto aina, mutta koska kopioinnin kesto voi tietomäärästä riippuen olla hyvinkin pitkä, se ei aina ole kannattavaa. Tosin nykyaikaisten tallennusmedioiden kasvavat nopeudet ja kapasiteetit mahdollistavat joissain tapauksissa esimerkiksi päivittäiset (yön yli otettavat) täydet varmuuskopiot. (Backup4all 2012c.)

Täyden varmuuskopioinnin etuja on myös sen palauttamisen nopeus. Koska täysvarmistus kopioi suoraan tiedostot ja kansiot sekä täydellisen kansiorakenteen, sen palauttaminen on yksinkertaisinta ja nopeinta. Toisin kuin lisäys- ja eroavuusvarmistuksessa, tiedostojen palauttamiseen ei tarvita kuin yksi täysvarmistus. (Backup4all 2012c.)



Kuva 2. Täysvarmistus

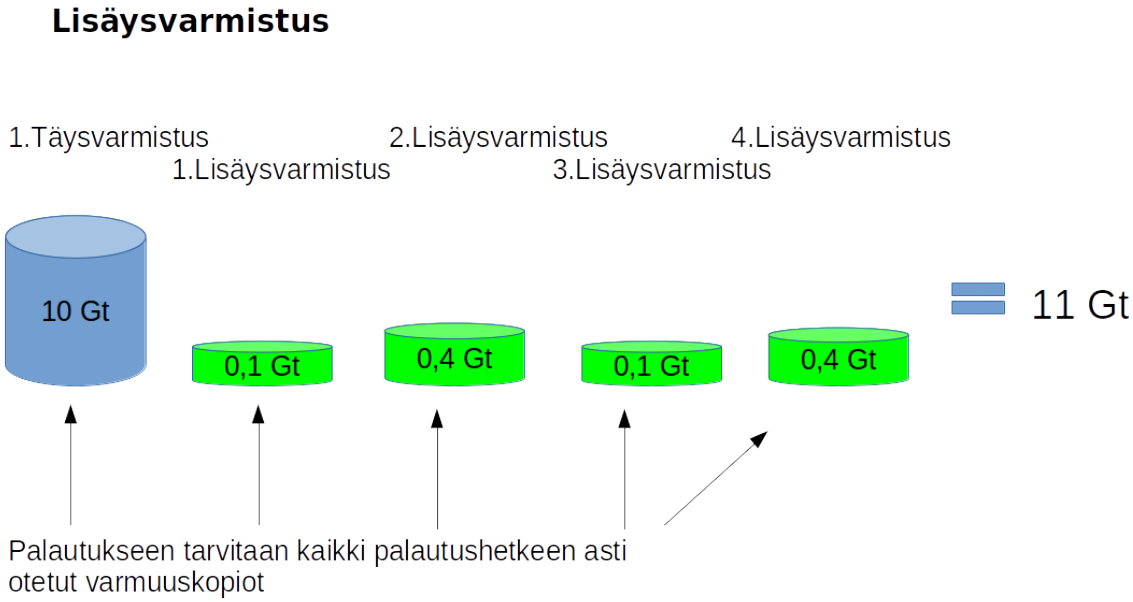
2.2.2 Lisäysvarmistus

Lisäysvarmistus (lisäyskopiointi, incremental-backup) tarkoittaa varmuuskopiointia, jossa varmuuskopioidaan viimeisen täys- tai lisäysvarmistuksen jälkeen lisätyt ja muokatut tiedot. Lisäysvarmistus kopioi talteen ainoastaan edellisen, minkä tahansa varmuuskopioinnin jälkeen muuttuneet tiedostot.

Lisäysvarmistuksen suurimpana etuna on sen ottamisen nopeus. Muihin varmuuskopiointimenetelmiin verrattuna lisäysvarmistus on nopein varmuuskopioinnissa ja se säästää myös tallennustilaa kopioiden ollessa pieniä. Toisaalta lisäysvarmistuksen palautus on hidasta, sillä viimeisimmän lisäysvarmistuksen lisäksi täytyy palauttaa yksi täysi varmuuskopiointi sekä kaikki sen syklin siihen asti otetut lisäysvarmistukset. Esimerkiksi palautus saattaa sisältää täysvarmistuksen lisäksi neljä lisäysvarmistusta (kuva 3). Varmistusohjelman täytyy prosessoida kaikki nämä varmuuskopiot, siksi palauttamiseen voi mennä enemmän aikaa kuin muissa menetelmissä. (Backup4all 2016a.)

Lisäysvarmistuksen aikana varmuuskopioitavien tiedostojen arkistointimääre asetetaan pois päältä, jolloin niitä enää varmuuskopioida seuraavan lisäysvarmistuksen yhteydessä. (Jaakohuhta 2011, 295.)

Koska lisäysvarmistus tarvitsee kaikki edelliset lisäysvarmistukset täysvarmistuksen lisäksi, yhdenkin lisäysvarmistuksen korruptoituminen tai häviäminen tekee koko varmuuskopion palautuskelvottomaksi. Tämän takia varmuuskopiointisykli olisi hyvä pitää melko lyhyenä.

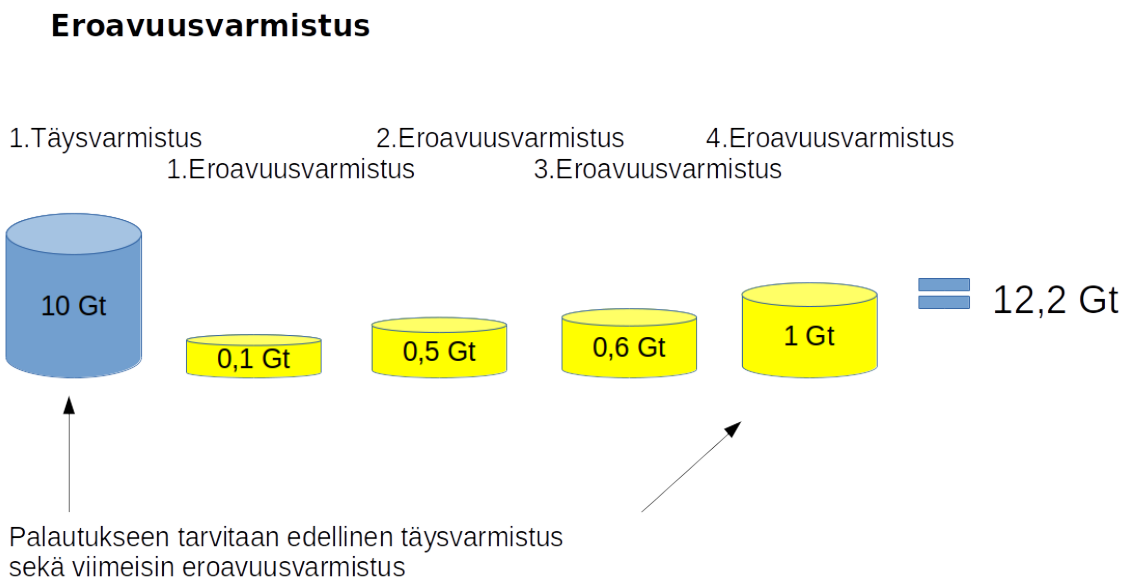


Kuva 3. Lisäysvarmistus

2.2.3 Eroavuusvarmistus

Eroavuusvarmistuksessa (differential backup, eroavuuskopiointi) varmistetaan lisäysvarmistuksen tapaan viimeisimmän täydellisen varmuuskopion jälkeen lisätyt ja muutetut tiedostot, mutta se ei muuta arkistointimäärettä. Tämän vuoksi jokainen eroavuusvarmistus kopioi myös mahdollisten edellisten eroavuusvarmistusten varmentamat tiedostot. (Jaakohuhta 2011, 159.)

Eroavuusvarmistuksen etuna täysvarmistukseen on sen ottamisen ja palauttamisen nopeus sekä varmuuskopion pienempi koko. Eroavuusvarmistuksen koko kasvaa kuitenkin täysvarmistusten välissä, jolloin varmuuskopioiden yhteenlaskettu koko saattaa nousta suureksi. (Backup4all 2016b.)



Kuva 4. Eroavuusvarmistus.

2.2.4 Online, Near-line ja Offline

Online- ja offline-termeillä viitataan varmuuskopioiden viiveeseen tai saatavuuteen. Online tarkoittaa jatkuvasti saatavaa ja verkossa olevaa varmuuskopiota, esimerkiksi pilvipalvelua internetin yli tai omassa verkossa toimivaa NAS-palvelinta (Network Attached Storage). Ajallisesti ajateltuna online-varmuuskopio on reaaliaikainen kopio varmistettavasta datasta, esimerkiksi RAID 1 -tason peilaus kahden levyn välillä. (Rao & Nayak 2014, 264.)

Near-line-varmuuskopio on lähes identtinen online-varmuuskopioinnin kanssa, mutta varmuuskopion ja oikean datan välillä on lyhyt viive. Usein near-line-varmuuskopioi rinnastetaan offline-varmuuskopioon. (Rao & Nayak 2014, 264.)

Offline-varmuuskopioilla tarkoitetaan verkosta irrotettua ja paikallista mediaa kuten DVD-levyt, CD-levyt, nauha-asemat, ulkoiset kovalevyt jne. (Rao, U., Nayak, U. 2014. 265) Offline-varmuuskopioita voidaan käyttää online-varmuuskopioinnin kanssa samaan aikaan. Esimerkiksi toimiston tärkeimmät tiedostot varmuuskopioidaan päivittäin toimiston omalle NAS-palvelimelle sekä pilvipalveluun. Tämän lisäksi yritys ottaa viikoittaisia varmuuskopioita nauha-asemalle ja säilöö nauhat paloturvalliseen kassakaappiin.

2.2.5 Menetelmien vertailu

Eri menetelmiä voidaan vertailla kolmen erilaisen määreen avulla: varmuuskopioinnin ja palautuksen keston sekä varmuuskopion koon perusteella. Myös varmuuskopioitavan datan kriittisyys sekä laatu ja datan määrä vaikuttavat lopullisen varmuuskopiointimenetelmän valintaan.

Täysvarmistus on aina tehtävä vähintään yhden kerran ennen kuin muita varmistusmuotoja käytetään. Sitä voidaan käyttää myös päämenetelmänä ja ottaa täysvarmistuksia esimerkiksi päivittäin, jolloin muita varmistusmuotoja ei tarvita. Tuolloin varmuuskopioitavan datan määrä on oltava melko pieni, muuten varmuuskopiointi kestää kauan ja kopiot ovat kooltaan suuria (taulukko 1). Jos kriittistä dataa ei muokata tai luoda päivittäin voi varmistusikkunaa kasvattaa ja ottaa varmistuksia esimerkiksi vain joka toinen päivä.

Jos tärkeitä tiedostoja on melko vähän, voidaan niitä synkronoida jatkuvasti pilvipalveluun tai NAS-palvelimelle. Tuolloin tärkeimmistä tiedostoista löytyy käytännössä uusin versio.

Taulukko 1. Varmuuskopiointimenetelmien edut ja haitat

Varmuuskopiointi menetelmä	Varmistettavat tiedot	Edut	Haitat
Täysvarmistus	Koko varmuuskopioitava data.	Yksinkertainen ja nopein palauttaminen. Pienentää datan menetyksen riskiä.	Vaatii pidemmän varmistussyklin. Vaatii enemmän tallennustilaa.
Lisäysvarmistus	Edellisen varmistuksen jälkeen luodut tai muokatut tiedot.	Nopea varmuuskopiointi. Vaatii vähän tallennustilaa.	Hidas palauttaa. Seisonta-aika pidempi -> kustannukset suuremmat.
Eroavuusvarmistus	Edellisen täysvarmistuksen jälkeen luodut tai muokatut tiedot.	Nopea palautus. Lyhyt seisonta-aika -> kustannukset pienemmät.	Hitaampi varmuuskopiointi.

2.3 Tietojen palautus

Hävinneet tai vahingoittuneet tiedot voidaan palauttaa varmistustavasta riippuen joko varmistusohjelman avulla tai puhtaasti kopioimalla tiedostot takaisin. Tietojen palautus riippuu tuhon laajuudesta. Esimerkiksi koko toimiston tuhonneen tulipalon jälkeen tietojen palautus voi kestää huomattavan kauan. Pahimmillaan myös NAS-palvelin on tuhoutunut, jolloin data on tallessa ainoastaan pilvessä. Sieltä sen palauttamisen kesto riippuu internetyhteyden nopeudesta ja datan määrästä. Palautusta hidastaa myös kaikkien laitteiden hankinta ja uudelleen asennus.

Mikäli tieto häviää vain käyttäjän tietokoneelta esimerkiksi kovalevyn rikkoutumisen takia, se saadaan palautettua uudelle kovalevylle suoraan NAS-palvelimelta. Toinen vaihtoehto on mahdollinen ulkoiselle tallennusvälineelle tallennetusta varmuuskopiosta.

Tarkemmin tietojen palautuksesta valitun varmuuskopiointiohjelman avulla liitteessä 3.

3 TALLENNUSMEDIAT

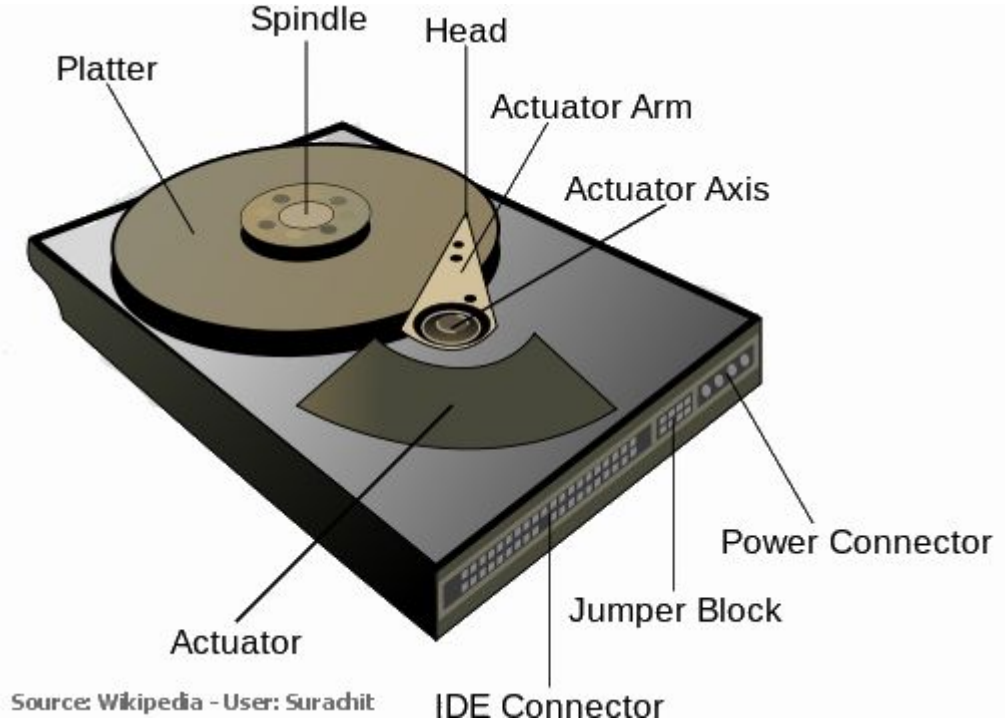
Varmuuskopiointi vaatii aina varmennettavasta kohteesta eriävän tallennusmedian. Erilaisia tallennusmedioita on esimerkiksi perinteinen kovalevy (HDD) sekä uudempi SSD-levy, nauha-asemat, muistikortit ja -tikut sekä optiset levyt.

3.1 Perinteinen kovalevy

Perinteinen kovalevy (HDD, Hard Disk Drive) on yksi suosituimmista tallennusmedioista. Tekniikka on peräisin 1950-luvulta, jolloin IBM valmisti 350 RAMAC -kovalevyn. Tämä laite käytti viittäkymmentä 24 tuumaista levyä, joille pystyttiin tallentamaan yhteensä 3,75 megatavua tietoa. Tästä tekniikasta kuitenkin luovuttiin ja myöhemmin 1980-luvulla standardoitiin 5,25 tuuman levyt, joita myöhemmin seurasi nykyäänkin käytössä olevat 3,5 sekä 2,5 tuuman kovalevyt. Kovalevyjen hinta on pudonnut ja kapasiteetti on kasvanut, nykyaikai-

set 3,5 tuuman levyt kykenevät 10 teratavun ja 2,5 tuumaiset 4 teratavun kapasiteettiin. (PCMag UK 2017.)

Kovalevy sisältää pyörivän metallilevyn, jossa on magneettinen päällyste (kuva 5). Levy pyörii laitteen sisällä ja lukupää liikkuu levyn reunalta toiselle tallentaen tietoa sähkömagneettisesti bitti kerrallaan. Levyltä luettaessa lukupäähän indusoituu heikko sähkövirta, joka tulkataan ohjauselektroniikan avulla luettavaan muotoon. (ACS Data Recovery 2017.)



Kuva 5. Kovalevyn komponentit (ACS Data Recovery. 2017.)

3.2 NAS-palvelin

NAS-palvelin (Network-attached storage, verkkolevy) käyttää tallennustilanaan kovalevyjä. Se on tiedostotason tallennusjärjestelmä, joka on lähiverkon kautta yhteydessä tietokoneisiin. NAS-palvelin sisältää vähintään yhden kovalevyn, mutta saatavilla on useita kovalevyjä sisältäviä palvelimia. Näissä voidaan käyttää RAID-teknologiaa jolloin voidaan esimerkiksi RAID 1:n avulla peilata yhden kovalevyn sisältö reaaliaikaisesti toiselle levylle.

3.3 SSD-levy

SSD-levy (Solid State Drive) tarjoaa perinteistä kiintolevyä nopeamman tallennusmuodon. Nopeamman luku- ja kirjoitusnopeuden lisäksi SSD-levyt kestävät paremmin tärinää ja kolhuja eivätkä sisällä lainkaan liikkuvia osia. Huonona puolena SSD-levyissä on niiden rajoitettu ylikirjoitusten määrä. Yksittäinen solu kestää vain tietyn määrän kirjoitusta, jonka jälkeen solu lakkaa toimimasta. Tiedon lukeminen ei kuluta soluja.

SSD-levyt ilmestyivät markkinoille kannettavien tietokoneiden yleistyessä 2000-luvun alussa. Kooltaan ensimmäiset SSD-levyt olivat vain noin gigatavun kokoisia, mutta kapasiteetti on kasvanut jopa neljään teratavuun. Hintaero perinteiseen kovalevyyn on yhä suuri. Esimerkiksi lokakuussa 2017 Verkkokauppa.com myy 250 gigatavun 2,5 tuuman SSD-levyä (Samsung 850 EVO) hintaan 109,90 € ja 2 teratavun perinteistä 2,5 tuuman kovalevyä (Seagate BarraCuda) hintaan 99,90 €. Jos tästä lasketaan senttihinta gigatavua kohti saadaan, SSD-levyn luvuksi noin 44 snt/Gt ja HDD-levyn noin 5 snt/Gt. Vertailun vuoksi Verkkokauppa.com myy myös magneettinauhoja, joista esimerkiksi 3 teratavun uudelleenkirjoitettava HPE LTO-5-tallennusmedia maksaa 40,90 €. Tämä on noin 1,4 senttiä gigatavulta.

3.4 Magneettinauha

Magneettinauha on moniin muihin tallennusmedioihin verrattuna vanha tekniikka. Se kehitettiin yli 60 vuotta sitten, mutta se on onnistunut säilyttänyt asemansa luotettavuutensa sekä tallennuskapasiteettinsa ansiosta yhtenä yleisimmistä varmuuskopiointimedioista. Vuonna 2017 teknologiayhtiö IBM rikkoi uuden ennätyksen nauhatallennuksen kapasiteetissa ja sai tallennettua yksittäiselle nauhalle 330 teratavua pakkaamatonta tietoa (The Verge 2017). Magneettinauhojen yleinen käyttö perustuu siis sen luotettavuuteen sekä hyvään hinta-kapasiteettisuhteeseen. Nauha-asema ei sovellu hyvin jatkuvaan tiedon lukuun ja kirjoittamiseen sillä tieto on tallennettu pitkälle nauhalle, jota on aina kelattava haluttuun kohtaan. Varmuuskopiointiin ja arkistointiin magneettinauhat sopivat hyvin. Nauhat säilyvät pitkään, kestävät hyvin kolhuja yms. ja maksavat suhteellisen vähän.

3.5 Optiset mediat

Yleisimmät optiset mediat ovat CD (Compact disk), DVD (Digital video disk) ja Blu-ray -levyt. Näiden kapasiteetti vaihtelee levystä riippuen CD:n noin 700 megatavusta Blu-rayn 50 gigatavuun. Levyt ovat verrattain halpoja ja ne oikein säilytettynä kestävät vähintään 100 vuotta. (iFixit 2015; Järvinen 2009, 298 301 309.)

Optiset levyt kestävät melko hyvin erilaisia olosuhteita ja esimerkiksi vedellä ei ole niihin lainkaan vaikutusta. Ne tukevat kaikkia tiedostomuotoja vaikka usein niitä on käytetty musiikin, videon ja asennustiedostojen jakamiseen.

Blu-rayn kapasiteetti on ylivertainen CD:hen tai DVD:hen verrattun ja sitä kehitetään edelleen. Sony ilmoitti vuonna 2014 jatkavansa Bly-ray-levyn kehitystä yhdessä Panasonicin kanssa uudella Archival Disc -formaatilla. Archival Diskistä on tarkoitus muodostaa uusi standardi pitkän ajan varmuuskopioinnille. Sen kapasiteettia on suunniteltu kasvatettavan jopa 1 teratavuun, jolloin se muodostaisi varteenotettavan kilpailijan nauha-asemalle. (Sony.net 2014.; Techopedia.com s.a.)

Vaikka optiset levyt ovat kestäviä ja melko halpoja, voi niiden käyttö varmuuskopiointiin tulla kalliimmaksi kuin etävarmennus esimerkiksi pilveen. Lisäksi levyjen käyttö varmuuskopioinnissa on hankala automatisoida, sillä levy pitää asettaa koneeseen, suorittaa varmuuskopiointi ja poistaa levy erilliseen säilytyspaikkaan. Tämä sitoo aina henkilökuntaa varmuuskopiointiin.

4 VARMISTUSOHJELMAT

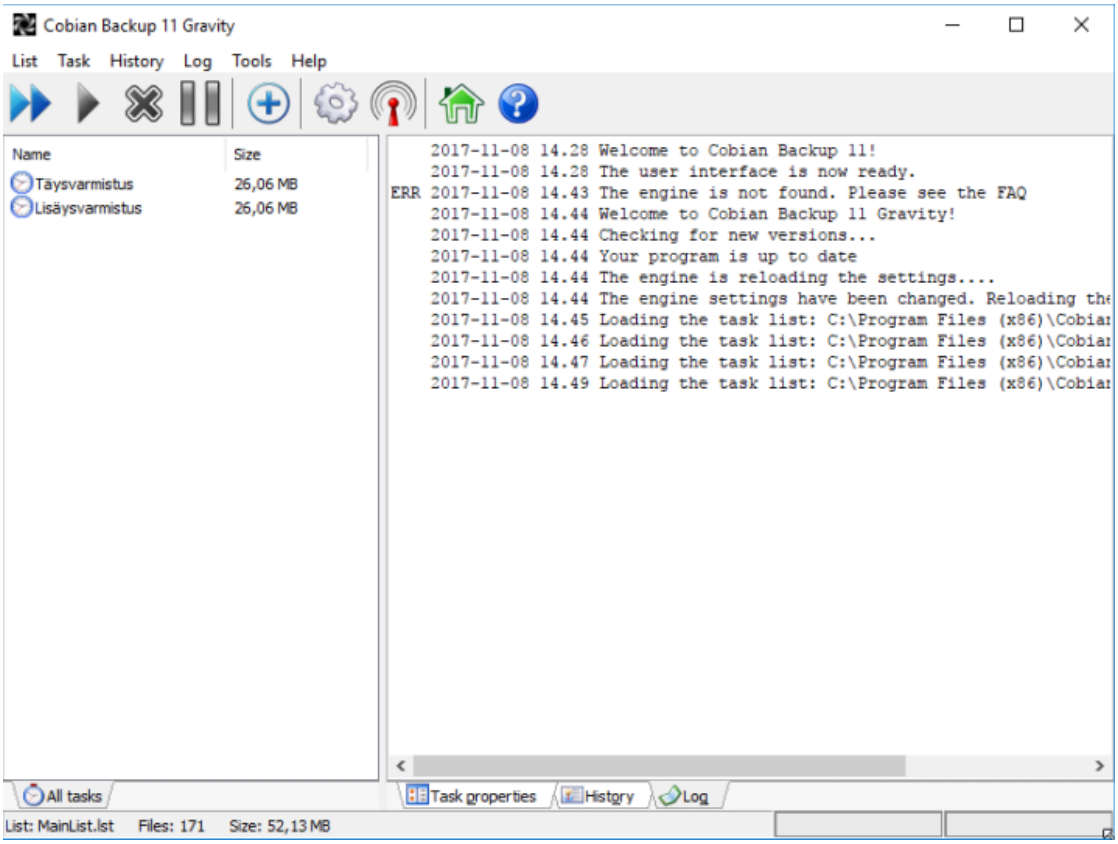
Varmuuskopiointi vaatii käytännössä aina erillisen varmistusohjelman, vaikka tiedostoja voidaan manuaalisesti kopioida paikasta toiseen ilman erillistä ohjelmistoa. Varmuuskopiointiin löytyy suuri määrä ohjelmia, joista opinnäytetyönä valmistuvaan varmuuskopiointipalveluun on tarkoitus etsiä monipuolinen ja ilmainen ohjelma, joten tässä työssä käsitellään vain ilmaisohjelmia. Ohjelmistot arvioidaan ominaisuuksien mukaan sekä testataan virtualisoidussa ympäristössä.

Yleisimpiä ilmaisia varmuuskopiointiohjelmia ovat Techradar.comin mukaan EaseUS Todo Backup free, Cobian backup ja Paragon Backup & Recovery. Muita ilmaisohjelmia on esimerkiksi Syncback free sekä Back4Sure. EaseUS Todo Backup free ei ole yrityskäytössä ilmainen, joten sen voi poistaa ehdokaslistalta.

Kaikissa testatuissa varmuuskopiointiohjelmissa, pois lukien Paragon Backup & Recovery, varmuuskopioiden palautus on tehtävä manuaalisesti Windowsin omalla tiedostonhallinnalla kopioimalla varmuuskopioidut tiedostot takaisin omille paikoilleen. Mikäli varmuuskopioidessa on valinnut tiedostojen pakkaamisen, täytyy pakattu tiedosto avata siihen soveltuvalla sovelluksella esimerkiksi ilmaisella 7-Zip-pakkausohjelmalla. Alkuun manuaalinen palauttaminen tuntui erikoiselta, mutta se itse asiassa yksinkertaistaa palautusta ja antaa vapauden valita vain halutut tiedostot palautettavaksi.

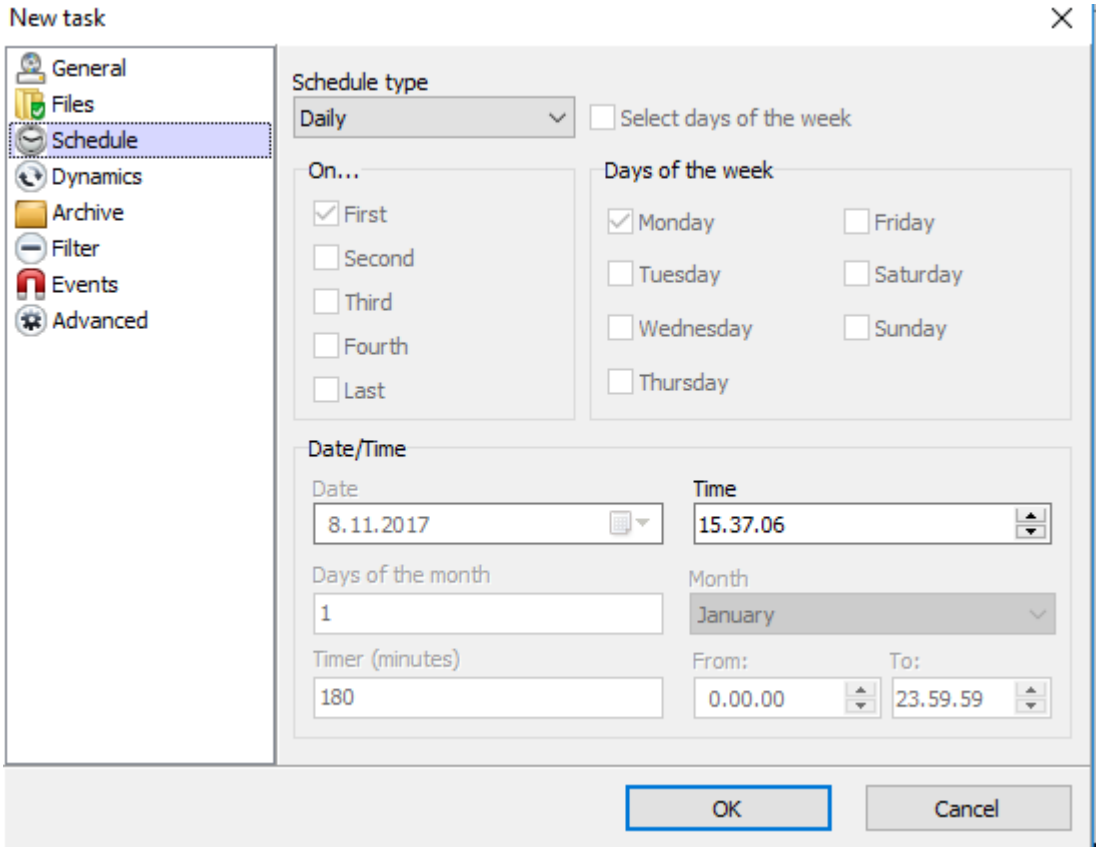
4.1 Cobian backup

Cobian Backup on kuubalaissyntyisen Luis Cobianin luoma varmuuskopiointiohjelma. Cobian backup tukee 7z- ja ZIP-pakkausta, levykuvan pilkkomista sekä salausta. Ohjelman käyttöliittymä on selkeä ja se tarjoaa paljon mahdollisuuksia yksilöidä varmuuskopiointi omiin tarpeisiin. Testattavaksi otettiin uusin versio 11 Gravity. (Softpedia 2017.)



Kuva 6. Cobian Backup 11 Gravity. Ohjelman pääikkuna

Cobian Backup 11 Gravity jää asennuksen jälkeen toimimaan taustalle. Asennuksen aikana voi valita haluaako asentaa ohjelman palveluna vai ajettavana ohjelmana. Siihen pääsee käsiksi Windowsin tehtäväpalkin ilmoitusalueelta klikkaamalla sen kuvaketta. Pääohjelmassa (kuva 6) voidaan asettaa uusi varmuuskopio useilla lisämääritteillä kuten varmuuskopiointimenetelmä, aikataulutus ja pakkaus sekä salaus. Asetukset ovat helposti saatavilla (kuva 7) ja niitä on paljon.



Kuva 7. Cobian Backup. Uuden varmuuskopiointityön asetuksista löytyy seikkaperäinen ajastus valikko

Varmuuskopioinnin ajastus on helppoa ja halutessaan ajastetun varmistuksen voi tehdä manuaalisesti. Ohjelma varmuuskopioi tiedostot sellaisenaan ja kansioi ne lähdekansion rakennetta noudattaen, kuitenkin lisäten kansion nimeen haluttuja tietoja kuten varmistusmenetelmän ja ajan. Aikaleiman asetuksia pääsee muuttamaan ohjelman omasta asetusvalikosta. Lisäksi Cobian Backup tarjoaa mahdollisuutta saada lokitiedostot omaan sähköpostiin jokaisen varmuuskopioinnin jälkeen.

Shadow Copy -palvelua käyttääkseen Cobian Backup vaatii .NET 3.5 Framework -ympäristön Windowsiin asennettuna ja päälle kytkettyinä.

4.2 Paragon Backup & Recovery Free

Paragon Backup & Recovery on Paragon Softwaren tekemä varmuuskopiointiohjelma. Paragon Software on ollut toiminnassa vuodesta 1994 ja se tarjoaa erilaisia ohjelmistoratkaisuja niin yritys- kuin kotikäyttöön. (Paragon Backup & Recovery 16 2017.)

Paragon Backup & Recovery Free tukee tärkeimpiä varmuuskopiointimenetelmiä ja siinä on runsaasti myös erikoisempia vaihtoehtoja. Esimerkiksi Paragon Backup & Recovery Free voi tallentaa varmuuskopion niin kutsuttuun backup capsuleen, joka on piilotettu loogisen levyn osio. Tämä osio pystyy toimimaan vaikka käyttöjärjestelmäosio vioittuisi. Lisäksi ohjelma tukee hot-processing-teknologiaa, joka mahdollistaa lukittujen tai käytössä olevien tiedostojen tai osioiden varmuuskopioimisen. (Paragon Backup & Recovery 16 2017.)

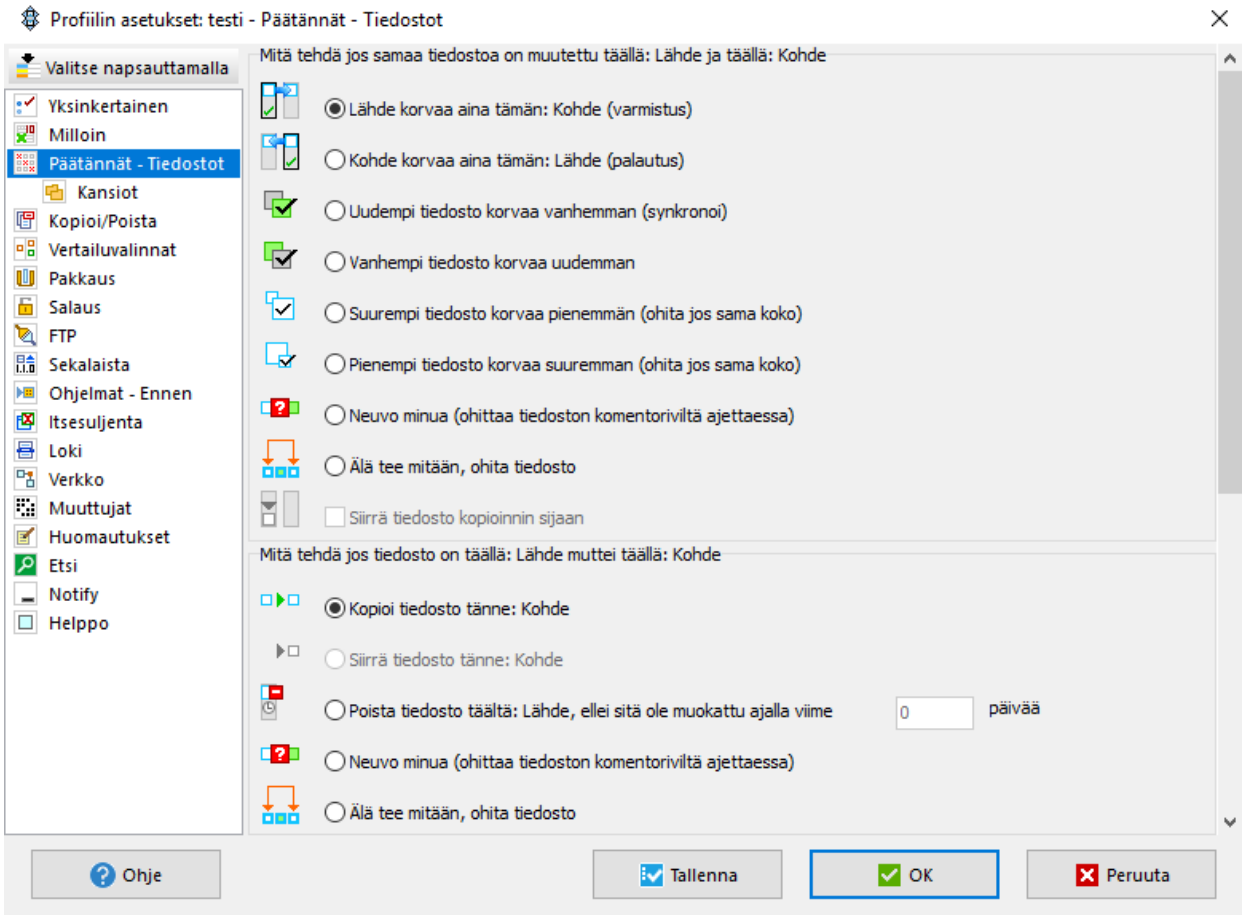
Paragon Backup & Recovery Free tulee ainoastaan Paragon Hard Disk Managerin mukana. Ainoana vertailtavista ohjelmista Paragon Hard Disk Manager pitää aktivoida viiden päivän kuluessa asentamisesta jotta kaikki ilmaisohjelman toiminnot tulevat käyttöön. Tämä tuntuu oudolta, sillä muissa testatuissa varmistusohjelmissa ei vastaavaa käytäntöä ole. Aktivointi on kuitenkin nopea ja vaivaton tehdä.

4.3 SyncBackFree

SyncBackFree on 2BrightSparkin valmistama, vuodesta 2003 asti käytettävissä ollut varmuuskopiointiohjelma. Ohjelmaa voidaan ajaa yksinkertaisessa tai edistyneessä tilassa, jolloin saadaan enemmän valintoja. (SyncBackFree 2017.)

SyncBackFree tukee varmuuskopioinnin lisäksi kansioiden synkronointia sekä peilausta. Synkronointi on kaksisuuntaista eli se synkronoi uudet ja muutetut tiedostot lähteen ja kohteen välillä molempiin suuntiin. Peilaus on yksisuuntainen ja se pitää kohdekansion täsmälleen lähteen mukaisena, tarvittaessa se myös poistaa kohteesta tiedostot mikäli ne on poistettu lähteestä.

SyncBackFree on käyttöliittymältään hieman kankea. Siinä uudet varmuuskopiointityöt luodaan profiileina ja jokainen profiili voi sisältää vain yhden kansion alikansioineen. Jos haluaa varmentaa useammasta eri sijainnista, joutuu tekemään jokaiselle kansiolle oman profiilin. Profiili luodaan yksinkertaisen wizardin eli apuohjelman avulla. Tämän jälkeen ohjelma siirtää suoraan profiilin asetuksiin jossa yksinkertainen tila tarjoaa vain muutamia asetuksia ja asiantuntijatila taas hieman liikaakin (kuva 8). Kuitenkin varmuuskopioinnin nimeäminen esimerkiksi päiväyksellä vaikutti mahdottomalta.



Kuva 8. SyncBackFree ja asiantuntijan valinnat

4.4 Back4Sure

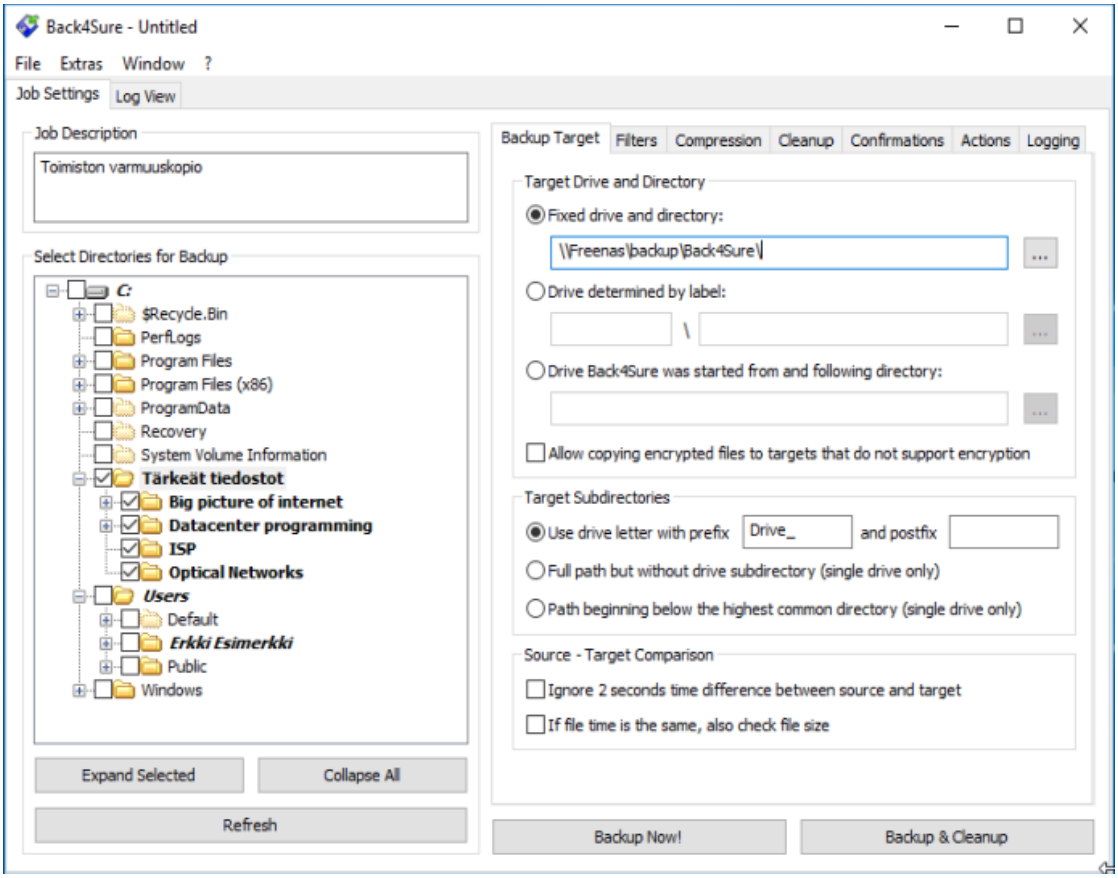
Back4Sure on Ulrich Krebsin luoma ilmaisohjelma tietojen varmuuskopiointiin. Se on erittäin pieni ja kevyt ohjelma ja siitä on saatavilla kiinteän asennuksen lisäksi ns. portable eli kannettava versio. Ohjelma pyrkii mahdollisimman yksinkertaiseen käyttöliittymään, mutta sisältää pieniä lisäominaisuuksia vaativimmille käyttäjille. Back4Sure tukee salausta, pakkausta sekä varmuuskopion ”siivousta” poistamalla tiedostot, jotka puuttuvat lähdekansiosta. Testattava ohjelmaversio oli 3.7.4. (Ulrich Krebs 2017.)

Back4Suren käyttöliittymä sisältää käytännössä vain pääikkunan, jossa varmuuskopiointityö asetetaan halutun mukaiseksi ja ajetaan. Ohjelma on suunniteltu myös ajettavaksi puhtaasti komentoriviltä, ohjelman mukana tulevasta ohjekirjasta löytyvät tarkat ohjeet sen käyttöön. Erillistä varmuuskopioinnin ajastusta ei ole, vaan halutun varmuuskopioinnin asetukset säädetään mieleiseksi, jonka jälkeen työtiedosto tallennetaan (kuva 9). Tämän jälkeen käynnis-

tetään Windowsin oma tehtävien ajoitus, johon luodaan uusi tehtävä. Tehtävä nimetään ja ajastetaan halutulla tavalla. Lopuksi määritetään ohjelmaksi Back4Sure.exe (löytyy oletuksena ”Program files” -kansiosta) ja lisätään argumenteiksi komentorivilläkin käytettäviä arvoja. Esimerkiksi seuraava rivi

```
-b -c -q -x ”C:\Program files\Back4Sure\Täysvarmistus.b4j"
```

avaa tallennetun työtiedoston ”Täysvarmistus.b4j” ja suorittaa varmuuskopioinnin ja siivouksen ilman käyttäjäinteraktiota sekä sulkee ohjelman automaattisesti työn valmistuttua.



Kuva 9. Back4Sure pääikkuna

Muuten selkeän ja helpon käyttöympäristön kanssa ajastus vaikuttaa työläältä, vaikka ohjelman luoja mainostaakin sen puuttumista yhtenä ominaisuutena (vähemmän taustaohjelmia). (Ulrich Krebs 2017.)

5 PILVITALLENNUS

Pilvitallennuksella tarkoitetaan datan tallentamista internetin välityksellä ulkoiselle palvelimelle. Kuluttajille tarjolla olevia palveluita ovat esimerkiksi Google Drive, Microsoft OneDrive, Dropbox ja Mega.

Pilvipalveluiden toimintaperiaatteet ovat samat, mutta eri palvelut tarjoavat hieman toisistaan poikkeavia ominaisuuksia. Esimerkiksi Google, Dropbox ja Microsoft tarjoavat toimisto-ohjelmia, jotka tallentavat kaikki muutokset välittömästi pilveen. Tästä käytetään termiä CDP, continuous data protection. Googlen Docs-tekstinkäsittelyssä tiedostoja käsitellään suoraan pilvessä ja tiedot tallentuvat käytännössä jokaisen kirjoitetun lauseen jälkeen. Tämä varmistaa kaikkein uusimman tiedoston säilymisen esimerkiksi sähkökatkon tai laiterikon sattuessa. Lisäksi työtä voidaan jatkaa suoraan toisella laitteella, eikä erillistä varmuuskopion palautusta tarvitse tehdä. Pilvitallennus Mega ei tarjoa toimistotyökaluja, vaan luottaa toimivaan ja hyvin salattuun tallennustilaan.

5.1 MegaSync

MegaSync on Kim Dotcomin johtaman Mega Limited -yhtiön luoma ohjelma, joka pohjaa toimintansa pilvitallenuspalvelu Megaan. Mega syntyi kun Dotcomin edellinen tiedostonjakopalvelu, Megaupload, suljettiin Yhdysvaltain oikeusministeriön toimesta.

Mega panostaa poikkeuksellisen vahvaan tiedon salaukseen. Palvelu salaa kaikki tiedot 128-bittisellä AES-salausjärjestelmällä (Advanced Encryption Standard), eikä edes Megan ylläpitäjät pääse näkemään palveluun ladattuja tiedostoja. Mega tarjoaa 50 gigatavua ilmasta tallennustilaa. Maksullisilla tileillä saa joko 200 Gt/4,99 €/kk, 1 Tt/9,99 € /kk, 4 Tt/19,99 €/kk tai 8 Tt/29,99 €/kk. (MEGA 2017.)

MegaSync on tietokoneelle asennettava ohjelma, joka synkronoi halutut tiedostot/kansiot Megan pilveen. Synkronointi on lähes realiaikaista, viive tulee ainoastaan yhteyden nopeudesta ja tiedonsiirtoajasta. MegaSync synkronoi kansiot molempiin suuntiin, jolloin pilvessä tai koneella tehdyt muutokset pei-

lautuvat suoraan toiseen sijaintiin. Kuitenkin vahingossa poistetut tiedostot löytyy pilven roskakorista. (MEGA 2017.)

5.2 Google Drive

Google Drive on Googlen pilvitallennus, joka tarjoaa käyttäjälle 15 gigatavua maksutonta tallennustilaa. Maksua vastaan saa joko 100 Gt/1,99 €/kk, 1 Tt/9,99 €/kk, 2 Tt/19,99 €/kk, 10 Tt/99,99 €/kk tai siitä eteenpäin 100 € lisämaksulla 10 teratavua lisää.

Google antaa ilmaisversiossaan loputtomasti tilaa Googlen omilla toimisto-ohjelmilla tuotetuille tiedostoille. Ohjelmistopaketti kattaa Docs-kirjoitusalustan, Slides-esitysalustan ja Sheets-taulukkolaskennan sekä mm. piirtotyökalun. Nämä ohjelmat ajetaan suoraan Googlen pilvessä ja muutokset tallentuvat välittömästi. Lisäksi tiedostojen jako ja muokkaus usean henkilön kesken on mahdollista (myös samanaikaisesti). Ohjelmat ovat hyviä ja yhteiskäyttöominaisuus toimii hyvin, mutta joitain esimerkiksi Microsoftin Wordin ominaisuuksia jää kaipaamaan.

Googlen Backup & Sync -ohjelmalla voidaan synkronoida tiedostoja tietokoneelta Googlen pilveen ja päinvastoin. Tiedostot kuitenkin synkronoituvat eri kansioihin molemmissa. Pilveen ilmestyy ”Tietokoneet” -valikko josta synkronoidut tietokoneet löytyvät. Huonona puolena ohjelmassa on se, ettei se tue verkon kautta liitettyjä levyjä kuten testiympäristön NAS-palvelinta.

5.3 Microsoft OneDrive

OneDrive on Microsoftin tuottama pilvipalvelu, joka sisältää tallennustilan lisäksi vahvan integraation Microsoftin muille tuotteille kuten Windows-käyttöjärjestelmälle sekä Office 365 -toimistopaketille. Se tarjoaa ilmaista tallennustilaa 5 Gt, mutta oppilaitosten opettajille ja opiskelijoille on tarjolla rajoittamaton tallennustila. OneDrive tarjoaa myös erikseen yrityksille suunniteltuja ratkaisuja esim. palvelupaketti 1 sisältää 1 teratavun/50,4 € vuodessa käyttäjää kohden tai rajoittamattoman tallennustilan 100,8 € vuodessa käyttäjää kohden. Lisäksi on saatavilla 1 teratavu tallennustilaa Office 365 -paketilla hintaan 126 € vuodessa käyttäjää kohden. (Microsoft. 2017.)

OneDrive ei kuitenkaan anna valita koneelta pilveen ladattavia kansioita erikseen vaan tarjoutuu lataamaan kuvat ja tiedostot automaattisesti pilveen. OneDrive luo koneelle oman OneDrive -kansion, joka synkronoituu pilven ja koneen välillä.

5.4 Dropbox

Dropbox, Inc -yhtiön luoma pilvipalvelu on testattavista palveluista vanhin. Sen kehitys aloitettiin vuonna 2008. Dropbox on käytettävissä, monen muun palvelun lailla, selaimen kautta, erikseen ladattavan ohjelman avulla tai mobiilisovelluksen kautta. Dropbox tarjoaa 2 gigatavua maksutonta tallennustilaa, jota voi kasvattaa suorittamalla pieniä tehtäviä tai kutsumalla ystäviä käyttämään palvelua. Dropbox tarjoaa yksityiselle käyttäjälle Plus ja Professional -tilit joissa molemmissa on 1 teratavu tallennustilaa, Plus 8,25 €/kk ja Professional 16,58 €/kk. Yrityskäyttöön löytyy Standard, jossa on 2 teratavua tilaa hintaan 10 €/käyttäjä/kk ja Advanced, jossa on rajoittamaton tila hintaan 15 €/käyttäjä/kk. Myös erikseen sovittava, suurille yrityksille tarkoitettu, Enterprise-tili on mahdollista tilata. (Wikipedia.org 2017.)

Dropbox-ohjelma on suunniteltu mahdollisimman helppokäyttöiseksi. Kirjautumisen jälkeen se luo tietokoneelle käyttäjän kansion alle uuden kansion, minne se lataa kaikki pilvessä olevat tiedostot ja päivittää sinne siirretyt tiedostot pilveen. Ohjelma mahdollistaa myös valokuvien ja videoiden siirtämisen automaattisesti kamerasta tai muusta ulkoisesta muistista. Ohjelma ei anna kuitenkaan valita verkkolevyllä olevaa kansiota synkronoitavaksi.

5.5 Pilvipalveluiden vertailu

Kaikkien pilvitallennuspalveluiden perustoiminnot ovat melko yhtäläiset. Tilaa saa yksityiskäyttöön ilmaiseksi nykymittapuulla riittävästi (pl. Dropbox). Yrityskäyttöön soveltuvia paketteja saa kaikilta yhtiöiltä ja niiden hinnat liikkuvat pitkälti samalla tasalla (Taulukko 2). Kaikki palvelut on kuitenkin suunniteltu hieman eri lähtökohdista. Esimerkiksi Mega panostaa käyttäjän yksityisyyteen, Dropbox helppokäyttöisyyteen ja Google sekä Microsoft tarjoavat omien tuoteryhmien helppoa integrointia toisiinsa.

Taulukko 2. Pilvipalveluiden hintavertailu

Palvelu	Maksuton tallennustila	1 Tt tallennustilan hinta	Lisätietoja
Mega	**50 Gt**	9,99 €/kk	Korostettu yksityisyys
Google Drive	15 Gt	9,99 €/kk	Sisäänrakennetut toimisto-ohjelmat
OneDrive	5 Gt	**4,2 €/kk**	Windows ja Office
Dropbox	2 Gt	8,25 €/kk	Kevyt Paper -toiminto

OneDrive on helppo valinta yritykselle, jolla on Office 365 käytössä. Se synkronoituu toimistosovelluksiin helposti ja takaa hyvän yhteensopivuuden Windows -järjestelmän kanssa. Google tarjoaa samaa, mutta hieman karsitulla toimisto-ohjelmistolla. Jos yritys ei tarvitse juuri Office 365 -sovelluksia, voi Google Drive olla hyvä vaihtoehto.

Dropboxin uusi Paper-toiminto on kuin kevyt versio Googlen Docsista. Se toimii lähinnä muistiinpanovälineenä, jonka voi jakaa muiden kanssa. Se ei kuitenkaan kilpaile toimisto-ohjelmistojen saralla Microsoftin tai Googlen kanssa. Dropbox luottaa helppokäyttöisyyteen ja se onkin yksi vanhimmista pilvipalveluista. Se onkin helppo valinta monelle, vain synkronointiohjelman yksilöintimahdollisuudet ovat puutteelliset.

Mega keskittyy puhtaasti luotettavan tallennustilan tarjoamiseen. Se antaa vertailluista pilvipalveluista eniten ilmaistilaa ja MegaSync-ohjelmisto on helppokäyttöinen sekä monipuolinen. Se pitää tiedostot jatkuvasti synkronoituna. Toisaalta se myös poistaa vahingossa poistetut tiedostot synkronoitavan kohteen päästä. Ne siirtyvät kuitenkin palvelun omaan roskakoriin, joten ne on palautettavissa vielä myöhemmin. Mega onkin hyvä valinta, jos ainoa tarve on pilvitallennus.

6 PALVELUN SUUNNITTELU

Varmuuskopiointipalvelu koostuu varmuuskopiointimenetelmä, varmistusohjelman, pilvitallennuksen sekä tallennuslaitteiden yhdistelmästä. Nämä valitaan ominaisuuksia vertailemalla sekä testaamalla virtuaalisessa ympäristössä.

6.1 Menetelmän valinta

Menetelmä tulee valita yrityksen varmuuskopioinnin tarpeen mukaan. Ympäristöjen ja olosuhteiden vaihdellessa on parempi valita yksi toimiva strategia, josta voidaan vaihtaa osia tilanteen mukaisesti.

Yleisesti laajassa käytössä on täysvarmistuksen ja lisäysvarmistuksen yhdistelmä, myös eroavuusvarmistus on yleinen. Varmuuskopiointipalvelun pohjaksi valitaan vähintään viikoittainen täysvarmistus ja päivittäiset lisäysvarmistukset. Varmistettavan datan määrästä riippuen varmuuskopiointipalveluun voidaan ottaa käyttöön myös eroavuusvarmistus. Tuolloin muuttuvaa dataa täytyy olla kymmeniä gigatavuja.

6.2 Ohjelmiston valinta

Ohjelmistojen ominaisuuksia ja käytettävyyttä testataan virtuaalisessa ympäristössä. Samalla voidaan testata pilvipalveluiden synkronointiohjelmia. Näistä helppokäyttöisimmät ja luotettavimmat ohjelmat valitaan varmuuskopiointipalveluun.

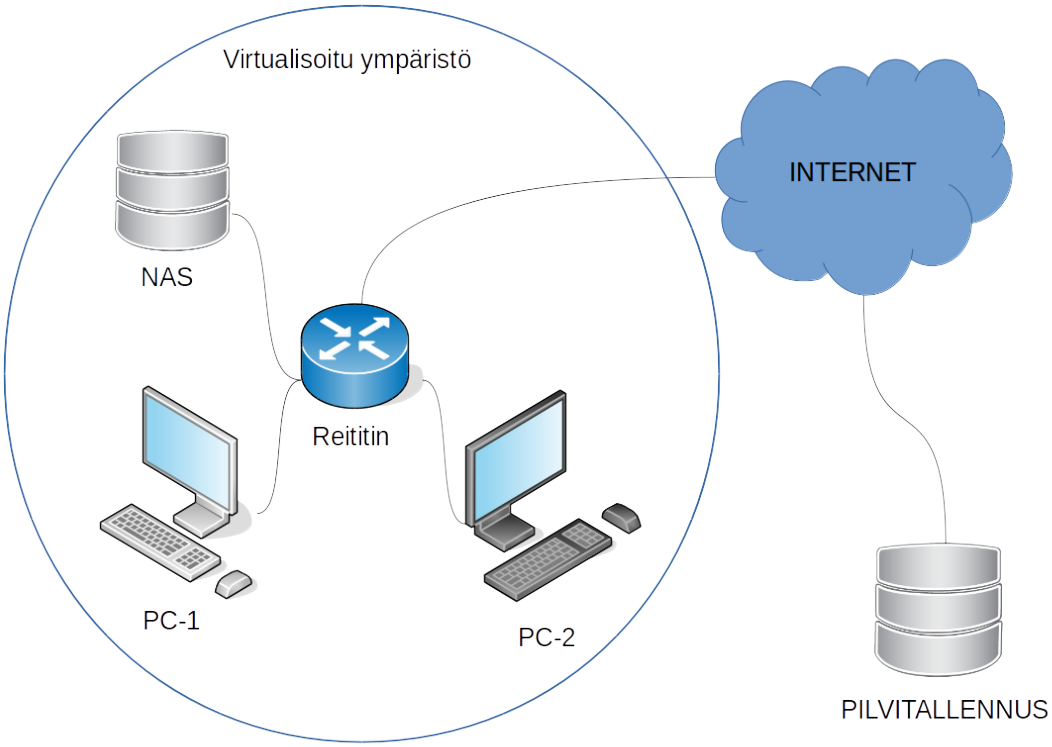
6.2.1 Ohjelmistojen testaaminen

Alkuperäinen suunnitelma oli toteuttaa ohjelmistojen testaaminen Kaakkois-Suomen ammattikorkeakoulun virtuaalilaboratoriossa, mutta erilaisten ongelmien takia testausympäristö vaihdettiin Linuxin päällä ajettavaan VirtualBox-virtualisointiohjelmistoon.

Työympäristön vaihdon takia erilaisten skenaarioiden testaaminen hankaloitui, mutta varmuuskopiointiohjelmien testaaminen helpottui. Testiympäristön kokoa rajoitti tietokoneen RAM-muisti, josta piti lohkaista jokaiselle virtuaaliko-

neelle oma osansa niin, että myös isäntäkoneelle jää käyttömuistia. Toisaalta skaalan kasvattaminen ei olisi tuonut lisäarvoa, sillä pääpaino oli varmennusohjelmien toimintojen testaaminen.

Skenaarion lähtökohta on pieni toimisto, jossa on kaksi pöytäkonetta, NAS-palvelin sekä internet-yhteys (kuva 10). Tämä toteutettiin VirtualBox-virtualisointiohjelmalla, jolla luotiin tarvittavat virtuaalikoneet sekä virtuaalinen verkko niiden väliin. Verkko toteutettiin käyttämällä VirtualBoxin asetuksista löytyvää NAT-verkkoa (Network Address Translation) sekä pelkkää NATia, jolla saadaan virtuaalisen lähiverkon lisäksi myös oikea internet-yhteys virtuaalikoneille. NAS-palvelimen alustana toimii FreeNAS-käyttöjärjestelmä ja pöytäkoneissa Windows 10. Lisäksi ympäristöön lisättiin pilvipalvelu, joista testattiin Google Drive, Microsoft OneDrive, Dropbox sekä MegaSync. Pilvipalveluissa käytettiin opinnäytetyön tekijän omia tunnuksia sekä maksuttomia tilejä.



Kuva 10. Ohjelmistojen testausympäristö

Tiedostojen jakaminen pilvipalveluun suoraan verkkolevyltä voi pilvipalvelusta ja verkkolevystä riippuen olla haastavaa. Esimerkiksi verkkolevyvalmistaja Synologyn oma Cloud Sync -palvelu mahdollistaa pilvitallennuksen ja verkkolevyn suoran interaktion. Se tukee mm. Google Drivea, Dropboxia ja OneDrivea, mutta Mega ei löydy vielä tuettujen listalta. Palvelun avulla varmuuskopioiden

siirtäminen pilveen helpottuisi, sillä ne voitaisiin ladata sinne öisin tietokoneiden ollessa sammutettuina. Mikäli haluaa kuitenkin käyttää tukematonta pilvipalvelua tai eri valmistajan verkkolevyä, voidaan synkronointi suorittaa pilvipalvelun omalla ohjelmalla. Tämä tosin vaatii pilvipalvelun synkronointiohjelman sisältävän tietokoneen jättämistä päälle synkronoinnin ajaksi.

Testaamisessa keskityttiin ohjelmistojen käytettävyyteen, tehokkuuteen sekä varmuuskopioinnin ajastettavuuteen. Varmuuskopiointi menetelminä käytettiin täys- ja lisäysvarmennusta. Lopulliseen varmuuskopiointipalveluun menetelmät valitaan tilanteen mukaisesti.

Toimistokoneiden varmuuskopioitaviin tiedostoihin kuului Windowsin ”Tiedostot”-kansio sekä C-aseman juuresta löytyvä ”Tärkeät tiedostot”-kansio, johon oli tallennettu tähän opinnäytetyöhön liittyviä tiedostoja. Varmuuskopiointi suoritetaan ottamalla varmuuskopiot edellä mainituista kansioista verkkolevylle (NAS-palvelimelle), josta ne siirtyvät pilvipalveluun. Mikäli yrityksellä olisi jaettuja tiedostoja vain verkkolevyllä, varmennetaan ne myös pilvipalveluun sekä ajoittain ulkoiselle tallennusmedialle kuten kovalevylle. Simuloidussa ympäristössä erillisen muistivälineen kuten nauhavarmistuksen tai ulkoisen kovalevyn käyttöä ei tarvitse testata sillä varmuuskopiointiprosessi on täysin sama.

Pilvipalvelut asennettiin vain toiselle Windows 10 -koneelle, koska sitä kautta ne pääsevät verkkolevyn tietoihin käsiksi. Varmuuskopiointiohjelmat sen sijaan asennettiin molempiin työpöytäkoneisiin, jotta niiden toimintoja voidaan testata samanaikaisesti.

6.2.2 Pilvipalvelun valinta

Pilvipalveluksi varmuuskopiointipalveluun valitaan Mega. Se soveltuu yleisesti parhaiten eri tilanteisiin. Vaikka siinä ei ollut vielä tukea NAS-palvelimilta synkronointiin, on mahdollista että verkkolevyvalmistajat alkavat tukea sitä tulevaisuudessa. Mikäli asiakasyritys erikseen tarvitsee esimerkiksi Googlen tai Microsoftin integraatiota omissa toimissaan, voidaan näistä jompikumpi valita pilvipalveluksi. Mikäli asiakasyrityksellä on jo pilvipalvelu, kannattaa se hyödyntää varmuuskopioinnissa, eikä tällöin erillistä pilvitallennusta tarvitse ottaa käyttöön.

6.2.3 Ohjelmiston valinta

Ohjelmistoista varmuuskopiointipalveluun valittiin Cobian Backup. Sen helppokäyttöinen ulkoasu sekä monipuoliset asetukset sopivat niin peruskäyttäjälle kuin vaativammallekin käyttäjälle. Se kykenee pakkaamaan tiedostot sekä salaamaan ja pilkkomaan ne. Ohjelma nimeää varmuuskopiot päivämäärän ja kellonajan mukaan sekä osaa poistaa vanhentuneet varmuuskopiot automaattisesti.

Se on suunniteltu vain varmuuskopiointiin, eikä sisällä mitään ylimääräisiä toimintoja kuten Paragon Hard Disk Manager. Sen käyttöliittymä on käyttäjäystävällinen ja se sisältää oman ajastuksen toisin kuin Back4Sure. SyncBackFree taas on täytetty erilaisilla ominaisuuksilla, mutta yksinkertaisimpien toimintojen (kuten varmuuskopioiden nimeäminen) ei onnistu.

6.3 Välineiden valinta

Laitteiston valintaan vaikuttaa niiden tallennuskapasiteetti, vikaherkkyys sekä hinta. Hintavertailu suoritetaan Verkkokauppa.comin verkkosivuilta.

Magneettinauha on säilyvyydestään ja hinnastaan huolimatta pk-yritykselle liioiteltu varmuuskopiointiväline. Sen käyttö vaatii käytännössä aina ihmisen, toki kalliita itsevaihtavia nauha-asemiakin löytyy. Myös optisia medioita helpompia ja edullisempia varmennustapoja löytyy. Siksi varmuuskopiointipalvelun laitteistoksi valittiin verkkolevy eli NAS-palvelin sekä sitä tukemaan ulkoinen kovalevy, johon tiedostot ajoittain varmuuskopioidaan.

Verkkokaupasta löytyy verkkolevyjä kymmenittäin eri hintaluokissa. Halvimmillaan verkkolevyn saa hieman alle 100 eurolla (Buffalo LinkStation 220DE ilman kovalevyjä) ja kallein maksaa yli 7 500 euroa (Buffalo TeraStation 7120r Enterprise 48 Tt). Yrityskäyttöön tarvitaan vähintään kahdella kovalevyllä varustettu verkkolevy, joka tukee RAID-tekniikkaa. (Verkkokauppa.com 2017a.)

Asiakasyritys saa valita haluamansa NAS-palvelimen itse, mutta varmuuskopiointipalveluun on katsottu jo sopivat palvelimet. Pienempää datamäärää tal-

lettaessa riittää Buffalo LinkStation 520. Se tukee maksimissaan 2 x 3 Tt:n kovalevyjä sekä RAID tasoja 1 ja 0. Sen hinta Verkkokauppa.comissa oli kirjoitushetkellä 304,90 € (Verkkokauppa.com 2017b.)

Suurempaan tarpeeseen asiakasyritykselle voidaan hankkia Buffalo TeraStation 5410DN 12 Tt:n verkkopalvelin. Sen hinta on kirjoitushetkellä Verkkokauppa.comissa 998,90 €. Se tukee RAID-tekniikkaa (0, 1, 5, 6 ja 10) sekä varmuuskopiointia toiselle laitteelle. (Verkkokauppa.com 2017c.)

Parempaa vikasietoisuutta tavoiteltaessa voi asiakasyritys ostaa myös toisen NAS-palvelimen, joka sijoitetaan toisaalle ja jolle peilataan toisen verkkolevyn tiedot.

7 PALVELUSUUNNITELMA

Palvelusuunnitelma määrittelee jokaisen asiakkaan yksilöidyt menetelmät ja välineet. Se sisältää myös ohjeet varmuuskopioinnin käyttöönottoon sekä ohjeita vikasietoisuuden lisäämiseksi.

7.1 Palvelun komponentit

Varmuuskopiointipalvelu koostuu komponenteista. Nämä komponentit valitaan asiakasyrityksen tarpeen ja olemassa olevan toimintaympäristön mukaan seuraavaksi esitettävien kysymysten avulla.

Ensimmäinen kysymys: ”Kuinka suuri määrä varmuuskopioitavaa dataa asiakkaalla on?” Tämä määrittää varmuuskopiointimenetelmän ja tarvittavan laitteiston kapasiteetin. Perusstrategia varmuuskopiointipalvelussa on joko päivittäiset täysvarmistukset tai viikoittaiset täysvarmistukset päivittäisten lisäys- tai eroavuusvarmistusten kanssa.

Kaikesta varmuuskopioitavasta tiedosta ei usein muutu päivittäin kuin pieni osa. Varmuuskopiointipalvelun kannalta on tärkeä tietää kuinka suuri määrä dataa täytyy varmuuskopiota kokonaisuudessaan ja kuinka suuri osa siitä muuttuu päivittäin. NAS pystyy kyllä tallentamaan suuriakin määriä, mutta pilveen ladattaessa pitää huomioida internet-yhteyden nopeus. Esimerkiksi kau-

punkialueella yleinen 100 megatavun ADSL-yhteys saattaa antaa lähetysnopeudeksi vain 10 megatavua. Tuolla nopeudella 10 gigatavun tiedoston siirtäminen kestää noin 2,5 tuntia, 25 gigatavua noin 6 tuntia ja 50 gigatavua kestää noin 12 tuntia.

Mikäli varmuuskopioitavia tiedostoja on kokonaisuudessaan alle 25 gigatavua, voidaan käyttää päivittäistä täysvarmennusta. Jos kokonaisdatan määrä on noin 100 gigatavua, voidaan olettaa päivittäin muuttuvan datan olevan noin 5-10 gigatavua. Tuolloin voidaan käyttää täys- ja lisäysvarmistusten yhdistelmää tai jos datan palauttamisen nopeus on tärkeämpää niin täys- ja eroavuusvarmistuksen yhdistelmää. NAS-palvelin valitaan tarvittavan tallennustilan mukaan.

Toinen kysymys on ”Onko asiakkaalla pilvipalvelu?” Oletuksena asiakasyritykselle tarjotaan Megan tallennustilaa, mutta mikäli asiakkaalla on jo olemassa oleva pilvitallennus, käytetään sitä hyödyksi.

7.2 Ohjelman asennus ja konfigurointi

Kahviduuri Ay hoitaa varmuuskopiointipalvelun asentamisen. Ennen palvelun käyttöönottoa asennetaan NAS-palvelin yrityksen lähiverkkoon. Asennusohjeet tulevat valitun palvelimen mukana. Tarvittaessa ne voi ladata valmistajan verkkosivuilta.

Itse varmuuskopiointipalvelun asennus aloitetaan lataamalla tarvittavat asennustiedostot internetistä. Paketit kannattaa tallentaa esimerkiksi USB-tikulle tai verkkolevylle, jolloin ne on helpompi asentaa useammalle koneelle.

Pilvipalvelun synkronointiohjelmaa ei tarvitse asentaa kuin yhdelle tietokoneelle. Asennustiedosto löytyy Megan verkkosivuilta nimellä MegaSync. Ohjelma asennetaan oletusasetuksin ja asennuksen jälkeen avataan ohjelma. Kirjaudutaan sisään yritykselle luoduilla tunnuksilla, vaihdetaan varmuuskopioinnin kohde- ja lähdekansiot liitteessä 3 määritellyllä tavalla.

Varmuuskopiointiohjelma Cobian Backup asennetaan kaikkiin työasemiin, joissa käsitellään varmuuskopioitavia tiedostoja. Ennen asennusta on hyvä var-

mistaa, että Windowsin .NET Framework-komponentti on asennettu. Ensimmäisen asennuksen yhteydessä on hyvä muistaa valita asennusohjelmasta kohta ”Create a script for unattended installations”, jolloin asennusohjelma tallentaa valitut asetukset ja asennus seuraaviin koneisiin helpottuu. Muuten asennus kannattaa suorittaa oletusasetuksin.

Kun ohjelmat on asennettu, määritellään varmistusohjelman käyttöliittymässä uudelle varmuuskopioinnille halutut asetukset ja ajastetaan se. Ohjelma jää palveluna taustalle ja suorittaa halutut varmuuskopiot valittuina ajankohtina.

Varmuuskopiointipalvelun käyttöönottoon liittyvät toimenpiteet löytyvät liitteenä olevasta toimenpidekorteista (liite 2 ja 3).

7.3 Varmuuskopioinnin vikasietoisuus

Varmuuskopiointipalvelun tulee olla varmatoiminen ja luotettava. Sen on toimittava aina ja tietojen tulee olla täysin palautettavissa vahingon sattuessa. Vikasietoisuutta voidaan parantaa monella tavalla.

Jo esimerkiksi yrityksen tietokoneella voidaan käyttää kahta kovalevyä tärkeälle datalle ja ajaa niitä RAID 1 -tekniikkaa eli peilausta. Tuolloin vikasietoisuus kasvaa jo ensisijaisen tiedonkäyttäjän tasalla sillä kovalevyn hajoaminen ei vielä aiheuta tiedon menetystä.

Myös verkkolevyn kahdentaminen tuo lisävarmuutta. NAS kannattaa ensisijaisesti varustaa vähintään kahdella kovalevyllä jotka peilaavat toisiaan, mutta monen valmistajan NAS-palvelimet tukevat myös kahden palvelimen peilausta. Jos esimerkiksi yrityksellä on omassa toimistossa yksi NAS-palvelin ja rakennuksen kellarikerroksessa toinen saadaan huomattava lisäturva varmuuskopioille. Tuolloin yhden verkkolevyn hajoaminen esimerkiksi vesivahingon tai tulipalon takia ei hävitä ensisijaista varmuuskopiota kokonaan, toki pilvessä olisi vielä yksi kopio tiedoista.

8 JOHTOPÄÄTÖKSET

Opinnäytetyössä tutkittiin varmuuskopiointia yleisesti sekä eri menetelmien ja välineiden sopivuutta varmuuskopiointipalveluun. Aihe on ajankohtainen, sillä varmuuskopioinnin merkitys on muuttunut yhä tärkeämmäksi niin yksittäiselle ihmiselle kuin yrityksillekin. Monet yritykset käsittelevät päivittäin suuria määriä dataa joka on usein myös kriittistä. Tiedon häviäminen voi tarkoittaa suuria rahallisia menetyksiä ja pahimmassa tapauksessa yrityksen ajautumista konkurssiin. Luotettava varmuuskopiointi tulisikin olla kiinteä osa jokaisen yrityksen tietoturvaa. Opinnäytetyöni on ajankohtainen myös lisääntyvän verkkorikollisuuden, etenkin kiristysohjelmien takia.

Varmuuskopiointiin löytyy paljon ohjelmia ja välineitä sekä valmiita palveluita. Yritys voi halutessaan järjestää varmuuskopioinnin itse, mutta se voidaan myös ulkoistaa. Tärkeintä on turvata yrityksen tiedostot niin, että ne kestävät suuremmatkin onnettomuudet, varkaudet ja vahingot. Pelkästään yhdelle ulkoiselle kovalevylle tai USB-tikulle varmuuskopiointi ei riitä.

Opinnäytetyönä syntynyt varmuuskopiointipalvelu sopii hyvin pk-yrityksen käyttöön. Sitä voidaan mukauttaa yrityksen tarpeen mukaiseksi ja sen avulla voidaan automatisoida varmuuskopiointi kokonaan, jolloin inhimillisten virheiden mahdollisuus eliminoituu pois. Varmuuskopiointi suoritetaan päivittäin ja kopiot tallennetaan sekä verkkolevylle että pilvipalveluun, jolloin varmuuskopioinnin luotettavuus kasvaa.

Palvelu on helppo ottaa käyttöön. Se vaatii pienimmillään varmuuskopiointiohjelman ja pilvipalvelun asennuksen sekä varmuuskopioinnin asettamisen. Tarvittaessa verkkoon asennetaan myös verkkolevy tai kaksi sekä luodaan pilvipalveluun uusi tili. Varmuuskopiointi toimii tämän jälkeen täysin autonomisesti eikä vaadi kuin ajoittaista valvontaa. Varmuuskopiointipalvelu sopii hyvin myös yksittäisen ihmisen tiedostojen varmuuskopiointiin.

LÄHTEET

About Luis Cobian. s.a. About Luis Cobian. WWW-dokumentti. Saatavilla: http://www.cobiansoft.com/about.htm. [Viitattu 28.10. 2017].

ACS Data Recovery. 2017. Hard Drive Design and Operation - ACS Data Recovery. WWW-dokumentti. Saatavilla: https://acsdata.com/how-hard-drives-work/. [Viitattu 17.10.2017].

Backup4all. 2016a. WWW-dokumentti. Saatavissa: http://www.backup4all.com/kb/incremental-backup-118.html [Viitattu 10.10.2017].

Backup4all. 2016b. WWW-dokumentti. Saatavissa: http://www.backup4all.com/kb/differential-backup-117.html [Viitattu 10.10.2017].

Backup4all. 2012c. Backup types. WWW-dokumentti. Saatavissa: http://www.backup4all.com/kb/backup-types-115.html. [Viitattu 12.10.2017].

BestBackups.com. 2017. Online Backup vs Offline Backup – 2016 Edition - BestBackups.com. WWW-dokumentti. Saatavilla: https://www.bestbackups.com/online-backup-vs-offline-backup-2016-edition/. [Viitattu 5.10.2017].

Easy backup & flexible restoration! - Paragon Backup & Recovery 16. 2017.WWW-dokumentti. Saatavilla: https://backstage.paragon-software.com/free/br-free/. [Viitattu 6.11.2017].

Free Backup & Sync Software for Windows - SyncBackFree. 2017. WWW-dokumentti. Saatavilla: https://www.2brightsparks.com/freeware/freeware-hub.html. [Viitattu 6.11.2017].

Google Drive Account settings. 2017. WWW-dokumentti. Saatavilla: https://drive.google.com/settings/storage. [Viitattu 8.11.2017].

IFixit. 2015. Optical Disc Types. WWW-dokumentti. Saatavilla: https://www.ifixit.com/Wiki/Optical_Disc_Types [Viitattu 10.11.2017].

Jaakohuhta, H. 2011. Tietotekniikan sanakirja. Helsinki: Readme.fi.

Järvinen, P. 2009. Digiarkistointi. Helsinki: Docendo.

Kahviduuri. 2017. WWW-dokumentti. Saatavissa: http://kahviduuri.com/palvelut/. [Viitattu 20.11.2017].

MEGA. 2017. MEGA. WWW-dokumentti. Saatavilla: https://mega.nz/. [Viitattu 8.11.2017].

Microsoft. 2001. Chapter 14 - Data Backup and Recovery. WWW-dokumentti. Saatavilla: https://msdn.microsoft.com/en-us/library/bb727106.aspx. [Viitattu 11.10.2017].

Microsoft. s.a. Microsoft OneDrive. WWW-dokumentti. Saatavilla: https://onedrive.live.com/about/fi-fi/. [Viitattu 9.11.2017].

PCMag UK. 2017. SSD vs. HDD: What's the Difference? - Storage Devices - Reviews and Price Comparisons from PC Magazine. WWW-dokumentti. Saatavilla: http://uk.pcmag.com/storage-devices-reviews/8061/feature/ssd-vs-hdd-whats-the-difference. [Viitattu 17.10.2017].

Ransomware | Tietoja ja poisto-ohjeita. 2017. Ransomware | Tietoja ja poisto-ohjeita. WWW-dokumentti. Saatavilla: http://www.ransomware.fi/. [Viitattu 13.10.2017].

Rao, U., Nayak, U. 2014. The InfoSec Handbook. WWW-dokumentti. Saatavilla: http://link.springer.com/book/10.1007/978-1-4302-6383-8 [Viitattu 8.3.2017].

Sanastokeskus TSK ry. 2010a. WWW-dokumentti. Saatavissa: http://www.tsk.fi/tsk/termitalkoot/fi/hakemistot-267.html?page=get_id&id=ID215&vocabulary_code=TSKTT [viitattu 23.6.2017].

Sanastokeskus TSK ry. 2010b. WWW-dokumentti. Saatavissa: http://www.tsk.fi/tsk/termitalkoot/fi/hakemistot-267.html?page=resurssi&tiedosto=varmkopio.htm [viitattu 23.6.2017].

SearchDataBackup. 2015. What is data archiving? - Definition from WhatIs.com. WWW-dokumentti. Saatavilla: http://searchdatabackup.techtarget.com/definition/data-archiving. [Viitattu 24.8.2017].

SearchDataBackup. 2017. What is backup storage device? - Definition from WhatIs.com. WWW-dokumentti. Saatavilla: http://searchdatabackup.techtarget.com/definition/backup-storage-device [Viitattu 14.10.2017].

Softpedia. 2017. Cobian Backup Download. WWW-dokumentti. Saatavilla: http://www.softpedia.com/get/System/Back-Up-and-Recovery/Cobian-Backup.shtml. [Viitattu 8.11.2017].

Softpedia. 2017. Paragon Backup & Recovery Free Download. WWW-dokumentti. Saatavilla: http://www.softpedia.com/get/System/Back-Up-and-Recovery/Paragon-Drive-Backup-Express.shtml. [Viitattu 6.11.2017].

Sony.net. 2014. "Archival Disc" standard formulated for professional-use next-generation optical discs. WWW-dokumentti. Saatavilla: https://www.sony.net/SonyInfo/News/Press/201403/14-0310E/index.html [Viitattu 10.11.2017].

Synology Inc. 2017. DiskStation Manager - Knowledge Base. | Synology Inc. WWW-dokumentti. Saatavilla: https://www.synology.com/en-global/knowledgebase/DSM/help/CloudSync/cloudsync/. [Viitattu 9.11.2017].

Tandberg Data. 2011. Guide to Data Protection Best Practices. WWW-dokumentti. Saatavilla: http://www.tandbergdata.com/default/assets/File/white_papers/WP_BackupGuide.pdf. [Viitattu 24.8.2017].

Technopedia.com. (s.a.). What is a Blu-Ray Disk (BD)? - Definition from Techopedia. WWW-dokumentti. Saatavilla: https://www.techopedia.com/definition/2600/blu-ray-disk-bd [Viitattu 10.11.2017].

The Verge. 2017. IBM scientists have captured 330TB of uncompressed data into a tiny cartridge - The Verge. WWW-dokumentti. Saatavilla: https://www.theverge.com/2017/8/2/16074568/ibm-330-terabytes-record-uncompressed-data-cartridge-cartridge-tape. [Viitattu 17.10.2017].

Ulrich Krebs. 2017. UK's Homepage. WWW-dokumentti. Saatavilla: http://www.ukrebs-software.de/. [Viitattu 8.11.2017].

Verbatim-europe.co.uk. 2017. Backup data Survey | Verbatim. WWW-dokumentti. Saatavilla: http://www.verbatim-europe.co.uk/en/article/backup-data-survey/?con=42 [Viitattu 17.5.2017].

Verkkokauppa.com. 2017a. WWW-dokumentti. Saatavilla: https://www.verkkokauppa.com/. [Viitattu 20.11.2017].

Verkkokauppa.com. 2017b. WWW-dokumentti. Saatavilla: https://www.verkkokauppa.com/fi/product/60743/fxkvv/Buffalo-LinkStation-520-6-Tt-verkkolevypalvelin. [Viitattu 20.11.2017].

Verkkokauppa.com. 2017c. WWW-dokumentti. Saatavilla: https://www.verkkokauppa.com/fi/product/50402/hmgdb/Buffalo-TeraStation-5410DN-12-Tt-verkkolevypalvelin. [Viitattu 20.11.2017].

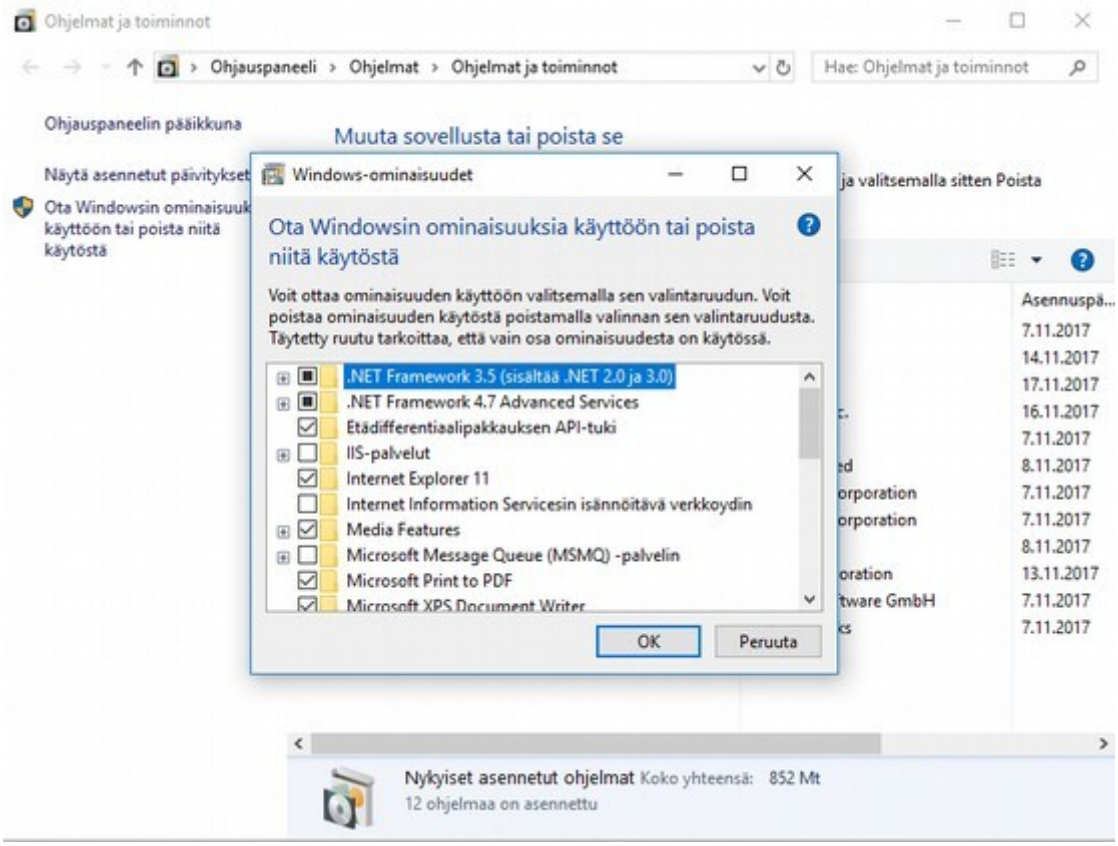
Wikipedia.org. 2017. Dropbox (service). WWW-dokumentti. Saatavilla: https://en.wikipedia.org/wiki/Dropbox_(service). [Viitattu 9.11.2017].

Liite 1/1

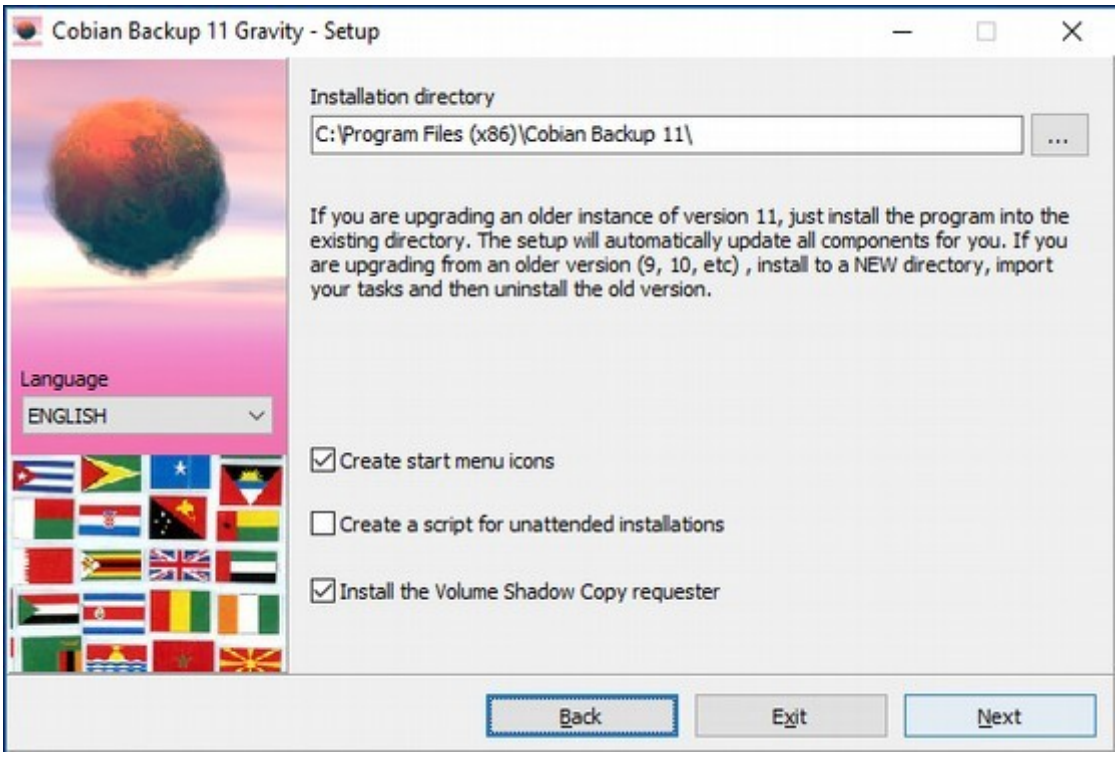
VARMUUSKOPIOINTIOHJELMAN ASENNUS

1. Ladataan varmuuskopiointiohjelman asennuspaketti internetistä, mieluiten valmistajan omilta sivuilta (http://www.cobiansoft.com/cobianbackup.htm). Asennusohjelman voi siirtää USB-tikulle tai verkkolevylle usean koneen asennusta helpottamaan.
2. Ajetaan asennusohjelma niissä koneissa, missä on paikallisesti varmuuskopioitavia tiedostoja. Jos varmuuskopioitavat tiedostot sijaitsee esimerkiksi verkkolevyllä, riittää asennus yhteen tietokoneeseen.
3. Otetaan Shadow copy -palvelua varten Windowsin .NET framework 3.5 käyttöön valitsemalla ohjauspaneelista ”Ohjelmat”, ”Ohjelmat ja toiminnot” ja sieltä ”Ota Windowsin ominaisuuksia käyttöön tai poista niitä käytöstä” (kuva 1).
4. Ohjelma asennetaan oletusasetuksin. Mikäli ohjelma asennetaan useampaan koneeseen, tulee ”Create a script for unattended installations” -kohta ruksia ensimmäisessä asennuksessa (kuva 2). Tämä luo asetustiedoston cbSetup.txt samaan kansioon mistä asennusohjelma ajettiin (esim. USB-tikku) ja uudelleen ajettaessa asennusohjelma käyttää oletuksena samoja asetuksia.
5. Asennustavaksi valitaan palvelu (service) ja syötetään käyttäjän kirjautumistiedot (kuva 3). Mikäli koneella ei ole domainia käytetään sen tilalla pistettä esim. ”.\Erkki Esimerkki”.
6. Seuraavaksi ohjelma asentuu. Lokin lopussa ei pitäisi olla virheilmoituksia. Mikäli virheitä tulee, tulee asennusloki tarkistaa ja varmistaa, että ohjelma asentui oikein.

Liite 1/2

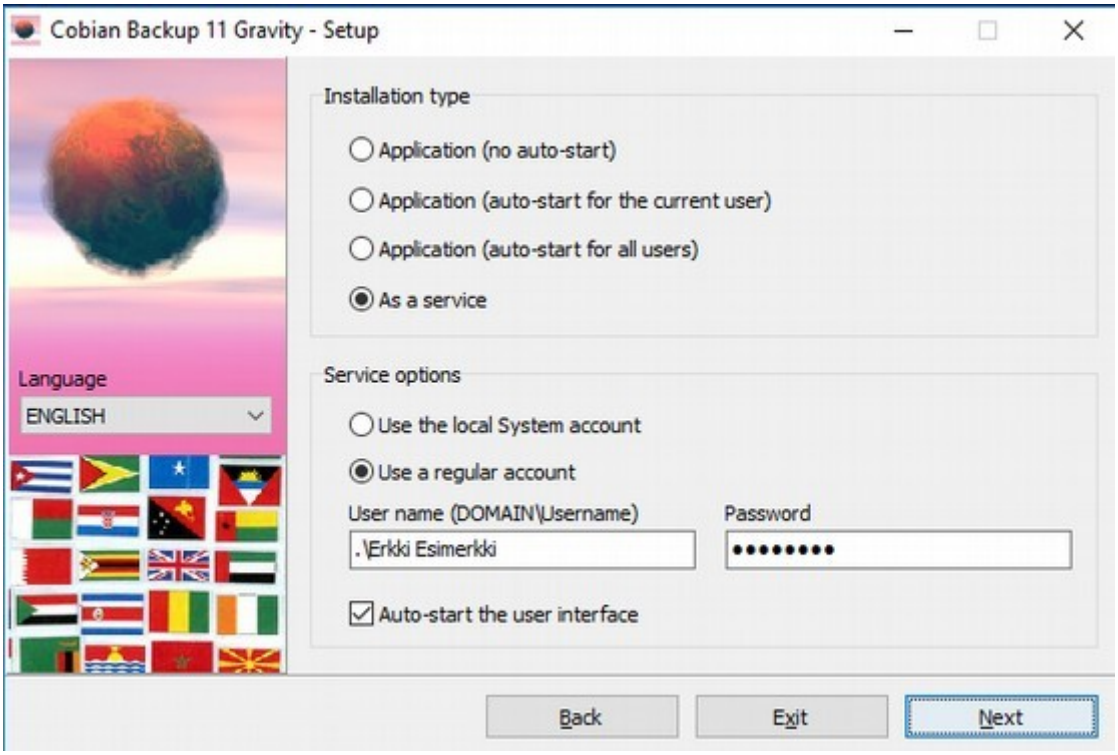


Kuva 1. Windows 10 .NET Framework 3.5 käyttöönotto.



Kuva 2. Cobian Backup asennus.

Liite 1/3

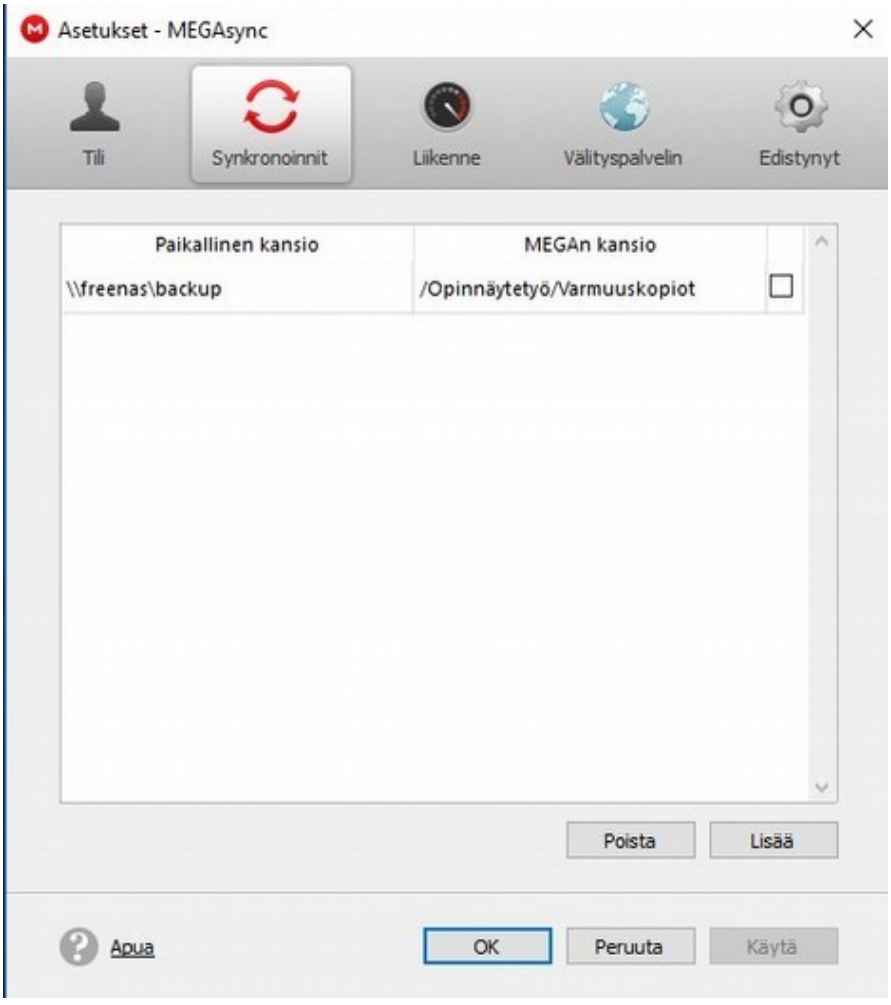


Kuva 3. Cobian Backup asennus.

Liite 2/1

PILVIPALVELUN KÄYTTÖÖNOTTO

1. Luodaan uusi tili asiakkaan nimissä Megan kotisivuilla (www.mega.nz/register). Tarvittaessa valitaan maksullinen palvelu tilantarpeen mukaan. Mikäli yrityksellä on jo pilvipalvelu käytössä, voidaan sitä hyödyntää, jolloin myös synkronointiohjelmaksi valitaan palvelun oma ohjelma.
2. Ladataan MegaSync -ohjelma Megan sivuilta valitsemalla valikosta ”Apps” ja ”Sync client”.
3. Asennetaan ohjelma yhteen verkkolevyyn yhteydessä olevaan tietokoneeseen.
4. Valitaan synkronoitavat kansiot ohjelman asetuksista (Kuva 1). Paikalliseksi kansioksi valitaan verkkolevyllä varmuuskopioinnit sisältävä kansio.
5. Pilvitallennus on nyt asetettu.



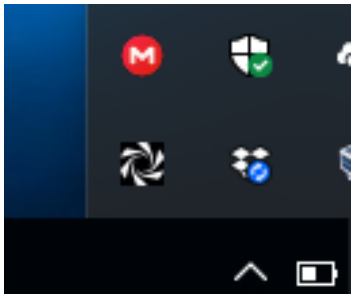
Kuva 1. MegaSync asetukset.

Liite 3/1

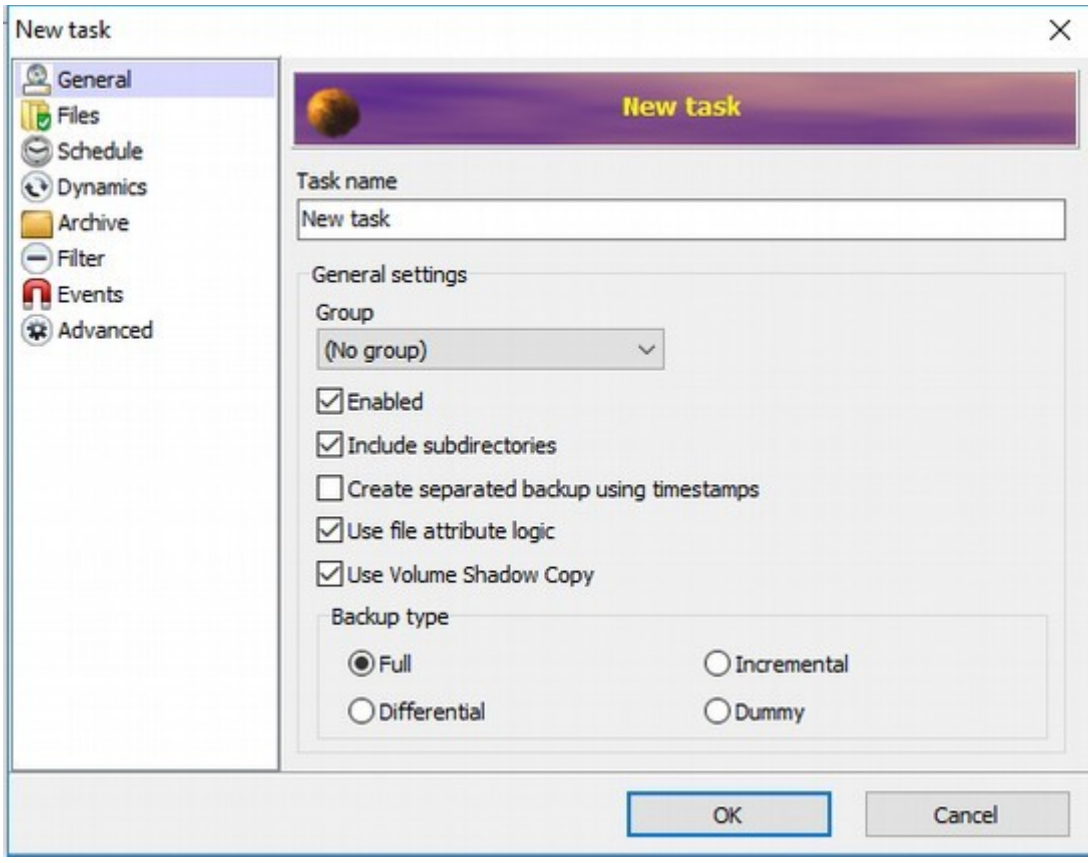
VARMUUSKOPIOINNIN ASETTAMINEN

1. Avataan Cobian Backup joko klikkaamalla ilmoitusalueelta sen kuvaketta tai käynnistä -valikon kautta
2. Klikataan plus-merkkiä työkaluriviltä tai Task -valikosta ”New task”.
3. Nimetään varmuuskopiointi. Nimi kannattaa valita esimerkiksi varmuuskopioitavan tietokoneen nimen mukaan. Tuolloin varmuuskopioiden palauttaminen on helpompaa yksittäiselle tietokoneelle. Lisäksi valitaan kohta ”Create separated backukp using timestamps” jolloin ohjelma luo aina uuden aikaleimalla nimetyn varmuuskopion.
4. Valitaan varmuuskopioinnin tyypiksi joko täysi (Full), inkrementaalinen (Incremental) tai differentiaalinen (Differential) (kuva 2). Mikäli varmuuskopiointi on suunniteltu vain täysvarmistusta käyttäen valitaan Full. Muuten valitaan tarvittava menetelmä.
5. Files -valikosta valitaan varmuuskopioitavat tiedostot ja kansiot sekä varmuuskopioinnin kohdekansio joka sijaitsee verkkolevyllä (kuva 3).
6. Ajastetaan varmuuskopiointi Schedule -välilehdellä. Ajastuksen tyypiksi valitaan viikoittainen (weekly) ja valitaan halutut viikonpäivät (kuva 4). Perusasetuksin valitaan arkipäivät maanantaista perjantaihin. Kellonajaksi kannattaa valita hetki jolloin asiakasyrityksen työaika päättyy, jolloin varmuuskopiointi ei häiritse työntekoa.
7. Dynamics -valikosta voidaan määrittää varmuuskopioinnin prioriteetti, mutta normaali prioriteetti on hyvä pitää asetettuna. Mikäli varmuuskopiointia on tarkoitus ajaa työajalla, voi prioriteettia laskea. Lisäksi voidaan määritellä kuinka monta täysvarmistusta ohjelma säilyttää ja voidaan määritellä esimerkiksi täysvarmistuksen otettavan aina perjantaisin (kuva 5).
8. Seuraavaksi määritellään varmuuskopioinnin pakkaus ja salaus (kuva 6). Zip -pakkaus on suoraan Windowsin tukema formaatti, mutta 7zip pakkaa tehokkaammin. Oletuksena kannattaa valita Zip. Valitaan vielä salausmenetelmä sekä salasana. Paras turva saadaan AES 256 bittisellä salauksella.
9. Varmuuskopiointi on nyt asetettu.

Liite 3/2

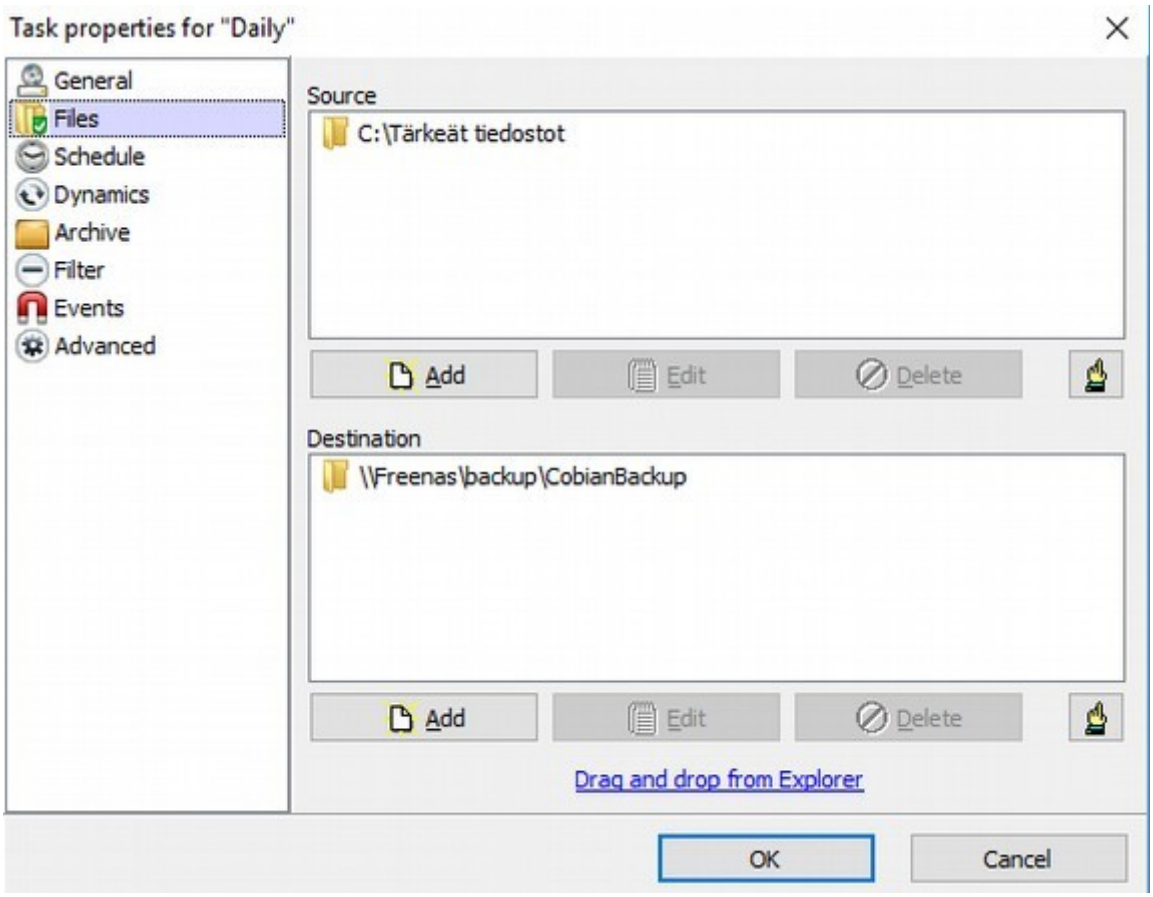


Kuva 1.

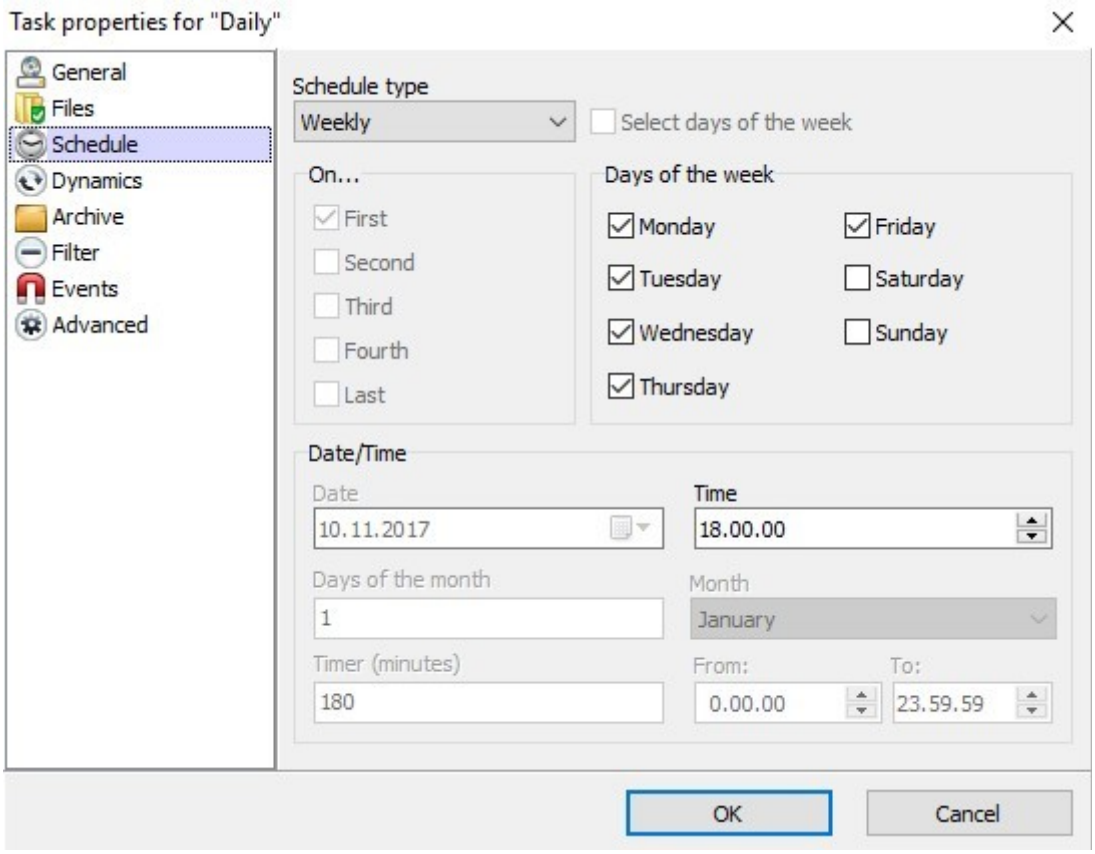


Kuva 2. Varmuuskopioinnin perusasetukset.

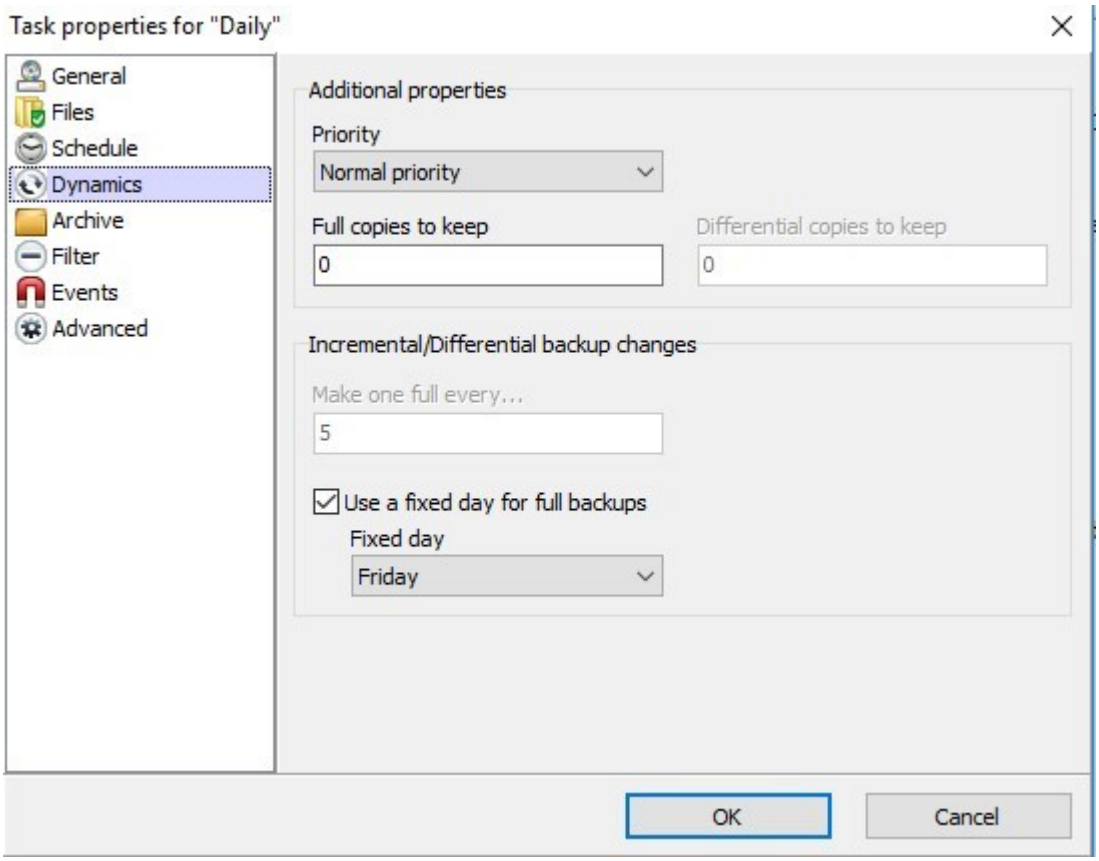
Liite 3/3



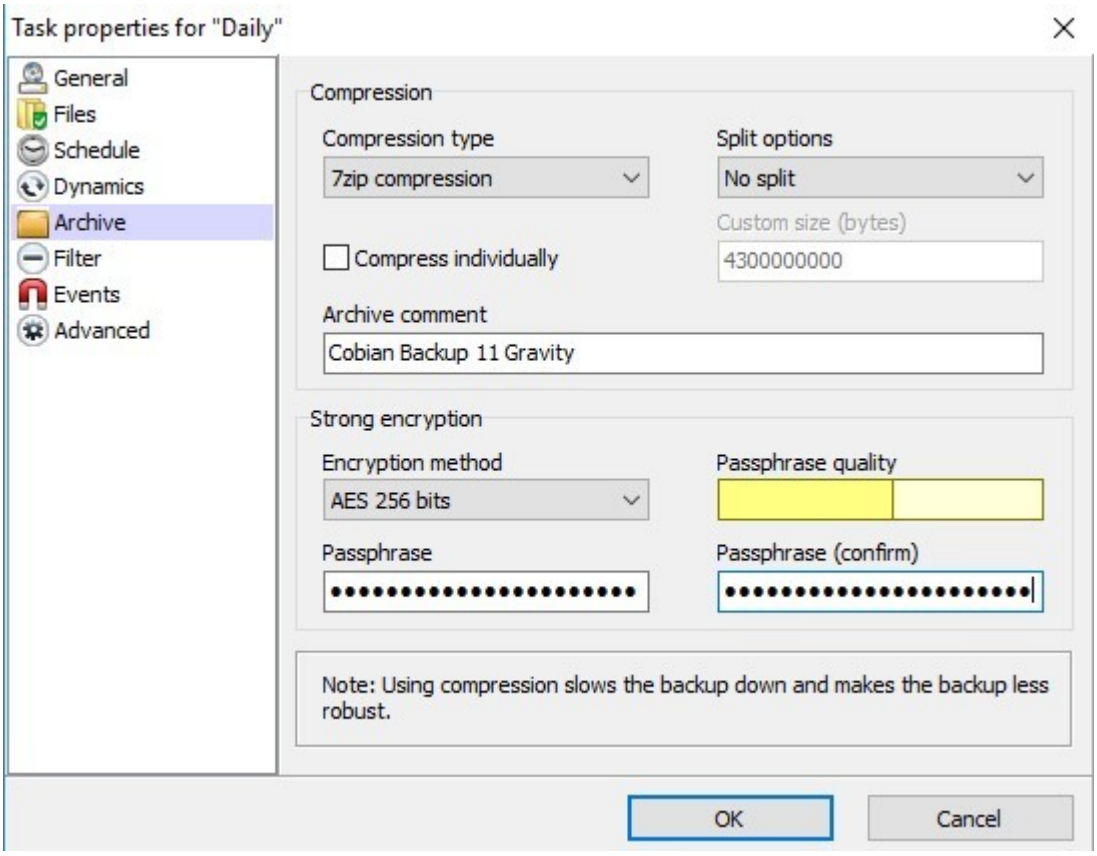
Kuva 3. Lähde- ja kohdekansioiden valinta.



Kuva 4. Varmuuskopioinnin ajastus.



Kuva 5. Varmuuskopioinnin lisäasetuksia.



Kuva 6. Pakkaus ja salaus.

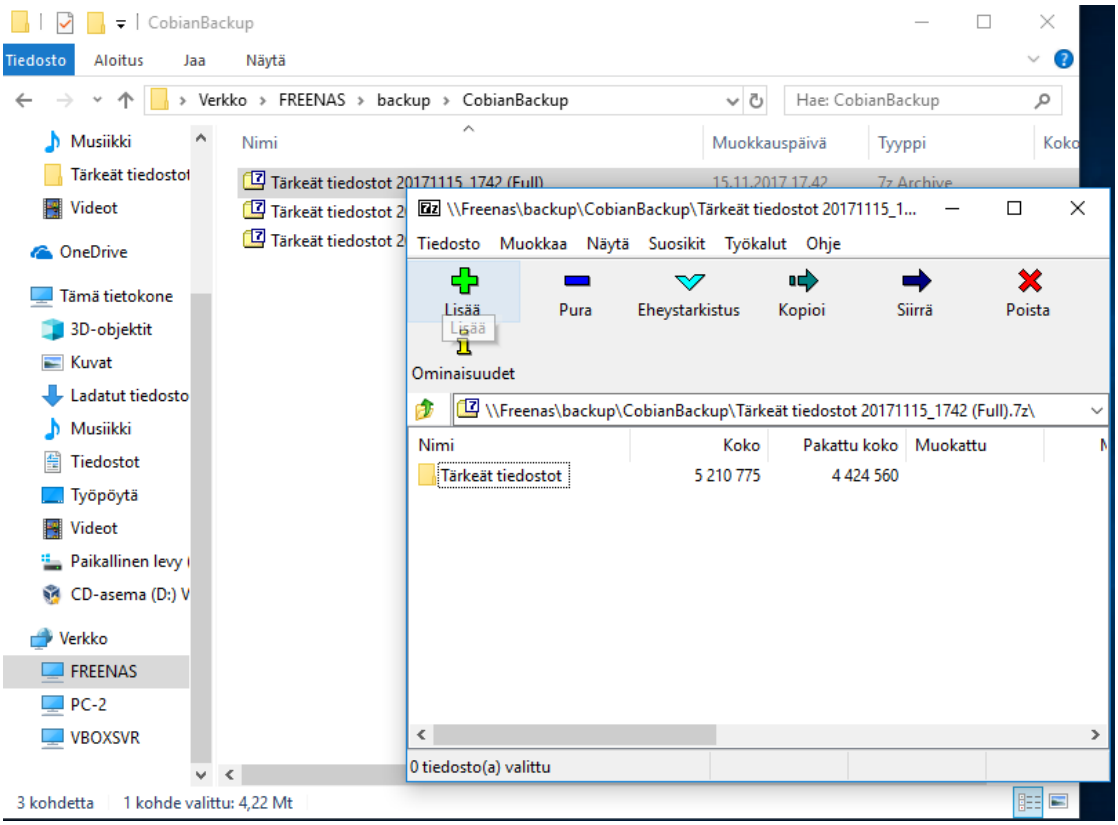
Liite 4/1

TIETOJEN PALAUTTAMINEN

Tietojen palauttaminen suoritetaan suoraan Windowsin resurssienhallinnan avulla.

Tietojen palauttaminen NAS-palvelimelta:

1. Avataan resurssienhallinta ja mennään verkkolevyn varmuuskopiot -kansioon.
2. Jos varmuuskopiot on pakattu zip-muotoon, avataan tiedosto Windowsin omalla pakkausohjelmalla. Jos tiedot on pakattu 7zip-muotoon, käytetään esimerkiksi ilmaista 7-zip -pakkausohjelmaa.
3. Puretaan tai kopioidaan kansio takaisin omaan sijaintiinsa.
4. Valmis.

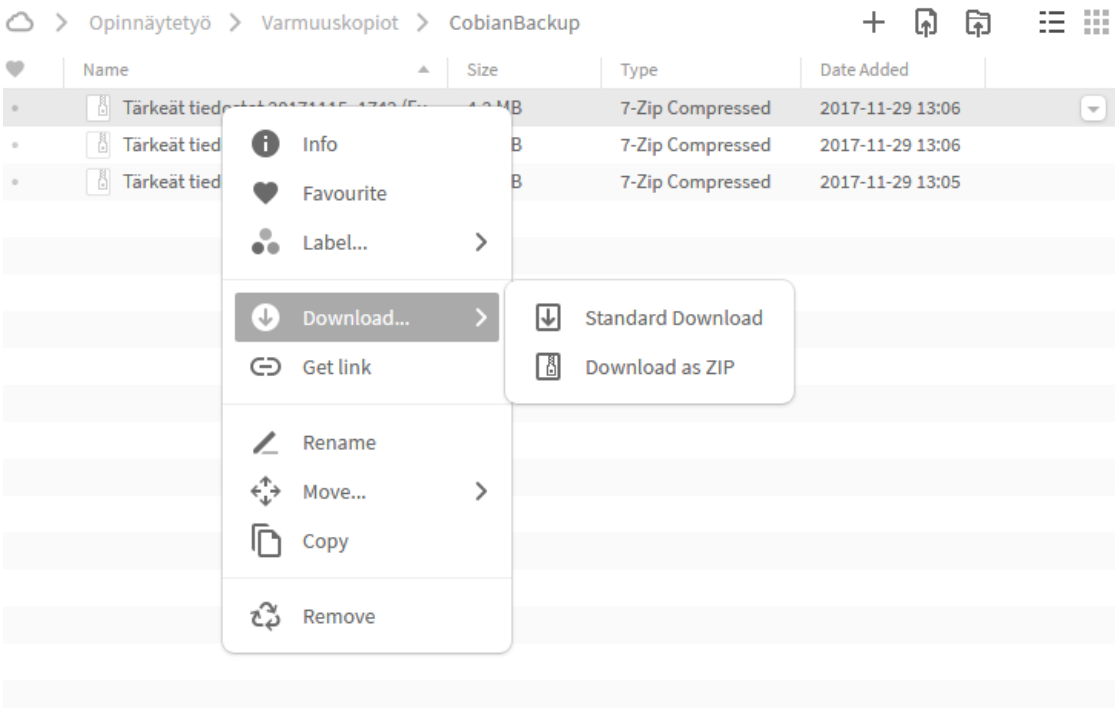


Kuva 1. Palauttaminen NAS-palvelimelta.

Liite 4/2

Tietojen palauttaminen pilvestä:

1. Kirjaudutaan Megan pilvipalveluun osoitteessa https://mega.nz/
2. Valitaan haluttu varmuuskopio ja klikataan sitä hiiren oikealla. Avautuvasta valikosta valitaan ”Download – Standard Download”.
3. Kun tiedosto on latautunut, puretaan tai kopioidaan tiedostot takaisin omaan sijaintiinsa.
4. Valmis.



Kuva 2. Megan pilvestä tiedoston lataaminen.